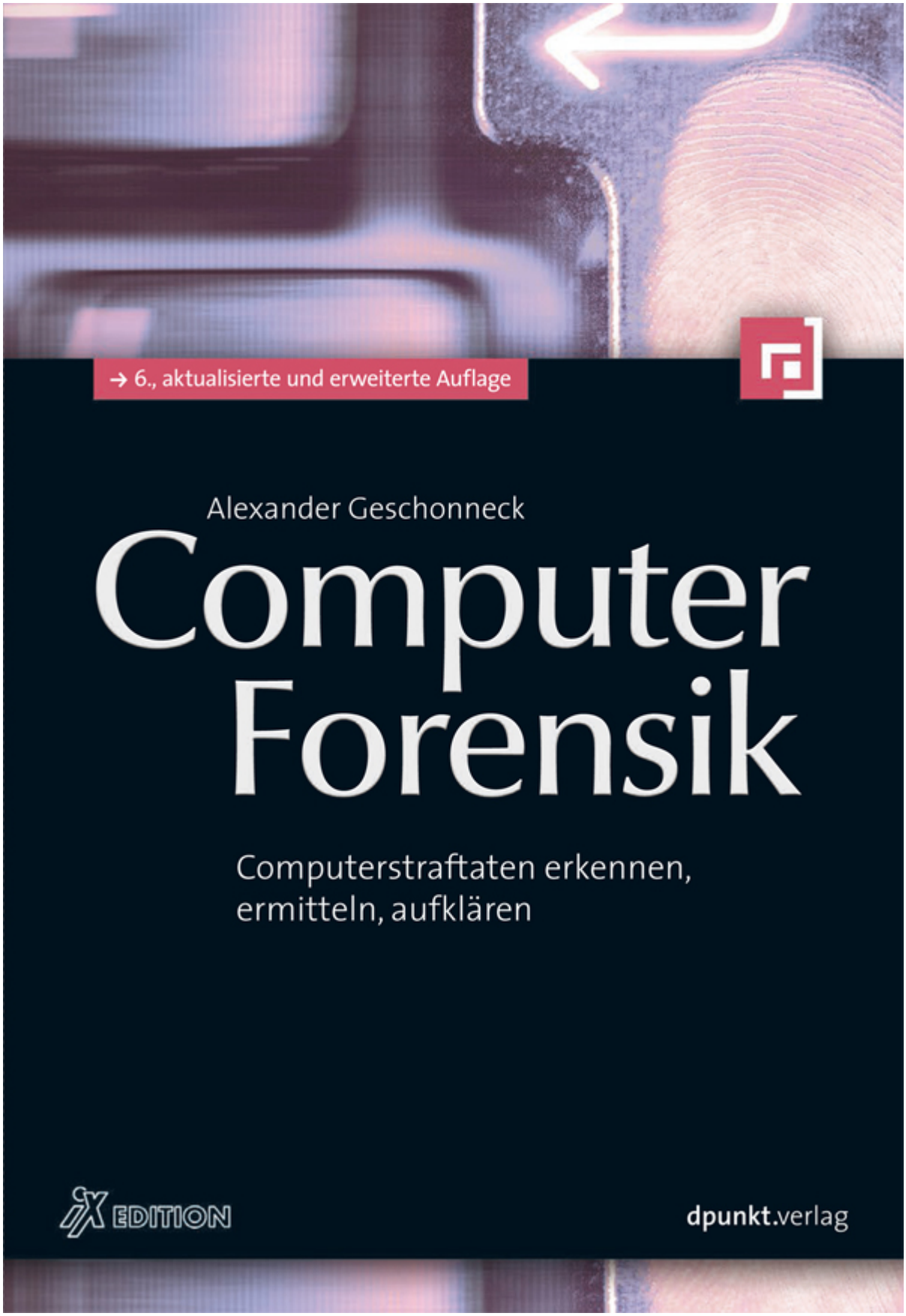

→ 6., aktualisierte und erweiterte Auflage
Alexander Geschonneck
Computer Forensik
Computerstraftaten erkennen, ermitteln, aufklären
iX EDITION
dpunkt.verlag

Inhalt

4 Einführung in die Computer-Forensik

Nach den vorbereitenden Kapiteln über Methoden der Angreifer und Vorbereitungsmaßnahmen für die potenziellen Opfer kommen wir nun zum Kernthema des Buches, der *Ermittlung*. Im Folgenden lernen Sie die wesentlichen Phasen eines Ermittlungsprozesses kennen. Das Kapitel liefert auch Informationen, welche Beweisspuren auf einem gehackten System gefunden werden, welche Daten sofort erfasst werden müssen bzw. in nachgelagerten Untersuchungsschritten ausgewertet werden können. Der vorletzte Abschnitt liefert Hinweise, wie die gefundenen Spuren schlussendlich im Zusammenhang zu bewerten sind. Häufige Fehler im Ermittlungsverfahren können dem letzten Abschnitt dieses Kapitels entnommen werden.

4.1 Ziele einer Ermittlung

Die Ziele einer forensischen Ermittlung nach einem Systemeinbruch oder einem anderen Sicherheitsvorfall sind in der Regel die folgenden:

- Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,
- Ermittlung des entstandenen Schadens nach einem Systemeinbruch,
- Identifikation des Angreifers,
- Sicherung der Beweise für weitere juristische Aktionen.

Die Umsetzung aller dieser Ziele steht und fällt damit, dass man die richtigen Daten von einem betroffenen System sammeln kann. Dies lässt sich auch in der folgenden Frage formulieren:

Wie stellt man sicher, dass so viele Informationen wie möglich von einem kompromittierten System gesammelt werden können, wobei der aktuelle Zustand bzw. Status dieses Systems so wenig wie möglich verändert wird?

Zur Beantwortung dieser scheinbar einfachen, aber in der Umsetzung recht komplexen Frage muss die Ursprungsfrage in Einzelaspekte aufgelöst werden:

- Wie wird der Angriff verifiziert?
- Wie sollten der kompromittierte Rechner und die zugehörige Umgebung gesichert werden?
- Welche Methoden können für die Sammlung von Beweisen verwendet werden?
- In welcher Reihenfolge sollen die Beweisspuren gesammelt werden?
- Wo sucht man nach Anhaltspunkten und wie können sie gefunden werden?

- Wie kann das Unbekannte analysiert werden?

Nachdem der Leser die beiden folgenden Kapitel gelesen hat, sollten die Antworten auf diese Fragen gefunden sein.

4.2 Anforderungen an den Ermittlungsprozess

Damit die vom Ermittler gewählten Methoden und Hilfsmittel auch vor Gericht Bestand haben, ist es wichtig, sich Gedanken zu machen, wie robust und sinnvoll diese sind. Ein Dritter, der eventuell nicht über den gleichen technischen Sachverstand und Erfahrungsschatz verfügt, muss den Tätigkeiten, die während der Ermittlung durchgeführt wurden, Glauben schenken können. Aus diesem Grund ist es wichtig, sich über allgemeine Anforderungen an die zum Einsatz kommenden Methoden und Hilfsmittel im Klaren zu sein. Zu folgenden Punkten sollte sich der Ermittler idealerweise im Vorfeld eine Meinung bilden:

- *Akzeptanz*

  Die vom Ermittler angewandten Methoden und Schritte müssen in der Fachwelt beschrieben und allgemein akzeptiert sein. Es ist immer schwierig, ein neues Verfahren oder Werkzeug einzusetzen, das in einschlägigen Publikationen oder auf Konferenzen noch keine Erwähnung gefunden hat. Idealerweise sollten andere professionelle Ermittler bereits damit gearbeitet oder positiv darüber berichtet haben. Sicherlich sind Quellen aus dem eigenen Land und Sprachbereich wünschenswert, aber nicht zwingend. Der Einsatz von neuen, noch kaum beschriebenen Methoden und Hilfsmitteln ist natürlich möglich. Es ist aber mit der Frage zu rechnen, warum man der Einzige ist, der damit arbeitet, wenn das Verfahren so gut sein soll.

- *Glaubwürdigkeit*

  Ein weiterer Punkt sind Anforderungen an die Funktionalität und Robustheit der Methoden. Diese sollten bei Bedarf nachgewiesen werden können. Es ist sicherlich immer schwierig, wenn man irgendein Tool mit Daten »füttert« und am Ende irgendwelche Ergebnisse »herauspurzeln«, deren Zustandekommen nicht nachvollziehbar ist. Dies ist besonders wichtig, wenn komplexe Werkzeuge und Methoden eingesetzt werden, deren Wirkungsweise vom Ermittler nicht verstanden werden und nicht plausibel erklärt werden können.

- *Wiederholbarkeit*

  Die im gesamten Ermittlungsprozess verwendeten Methoden und Hilfsmittel müssen bei Anwendung von Dritten wiederholbar sein. Dies bedeutet, dass eine dritte Person, die die gleichen Schritte durchführt, die gleichen Ergebnisse produziert.

- *Integrität*

  Im Rahmen des gewählten Ermittlungsprozesses dürfen die sichergestellen Spuren nicht unbemerkt verändert werden können. Es muss jederzeit demonstriert werden können, dass die Integrität der digitalen Beweise gewahrt bleibt.

- *Ursache und Auswirkungen*

  Die für die Ermittlung gewählten Methoden müssen es ermöglichen, logisch nachvollziehbare Verbindungen zwischen Personen, Ereignissen und Beweisspuren herzustellen.

- *Dokumentation*

  Jeder Schritt des Ermittlungsprozesses muss angemessen dokumentiert werden können.

4.3 Phasen der Ermittlung

Die Tätigkeiten, die im Rahmen der Ermittlungsphase des Incident-Response-Prozesses durchgeführt werden, lassen sich in weitere Zwischenphasen einteilen, wobei hier die letztendliche Ausprägung der einzelnen Phasen vom konkreten Ermittlungsfall abhängig ist.

- *Vorbereitung der Ermittlung*

  Zur gründlichen Vorbereitung auf die Untersuchung gehört unbedingt, dass eine entsprechende Autorisierung der Geschäfts- oder Organisationsleitung vorliegt. Dies gilt besonders für externe, nicht polizeiliche Ermittler. Forensische Untersuchungen, die auf keiner ordentlichen Grundlage beruhen, könnten sonst sehr schnell selbst Gegenstand von Ermittlungen sein. Arbeiten die Administratoren auf eigene Faust und verletzen dabei Persönlichkeits- bzw. Datenschutzrechte durch Einsicht in und Analyse von personenbezogenen Daten oder versuchen ihrerseits das vermeintliche Ursprungssystem des Angriffs zu attackieren, dann kann dies schnell zu einem Bumerang werden. Weiterhin gehört zur Vorbereitung, dass Auftrag und Ziel für die Ermittlung so klar wie zum Beauftragungszeitpunkt möglich von einer zeichnungsberechtigten Person definiert sind.

- *Schutz der Beweismittel*

  Dem Schutz der Beweismittel vor der Modifikation kommt in Bezug auf deren Gerichtsverwertbarkeit wesentliche Bedeutung zu. Hierzu zählt auch der Schutz der eigenen Untersuchungsumgebung und der verwendeten Betriebsmittel (siehe Abschnitt 6.2).

- *Imaging* (bitweise Kopie der Datenträger) *und Datensammlung* Abhängig vom konkreten Untersuchungsgegenstand werden in dieser Phase Informationen vom noch »lebenden System« gesammelt (siehe Abschnitt 4.7) oder es wird im Rahmen einer forensischen Duplikation ein Image der Datenträger des betroffenen Systems gezogen (siehe Abschnitt 4.8). Die gesammelten Daten werden nicht immer sofort ausgewertet.
- *Untersuchung und Bewertung der gewonnenen Informationen*

  Gerade die Analyse von Datenträger-Images findet im Nachhinein statt (siehe Kap. 5). Diese Untersuchungsphase ist zeitlich nur durch die äußeren Umstände eingeschränkt. Wichtig ist hierbei, dass die gewonnenen Daten nicht nur analysiert, sondern auch auf ihre Relevanz bewertet werden müssen.

- *Dokumentation*

  Da es sinnvoll ist, während aller Phasen eine schlüssige Dokumentation anzufertigen, dient die abschließende Dokumentationsphase der Zusammenfassung gewonnener Erkenntnisse und der Erklärung der Schlussfolgerungen. Die Erfahrung zeigt, dass Informationen und Tätigkeiten, die nicht sofort dokumentiert werden, wenn sie anfallen, niemals erfasst werden.

4.4 Das S-A-P-Modell

Die Secure-Phase

Nach dem sogenannten Secure-Analyse-Present-Modell (S-A-P-Modell) kann sich ein Ermittlungsprozess in drei große Phasen einteilen lassen. In der Secure-Phase werden alle Daten sorgfältig erfasst. Hierbei ist darauf zu achten, dass der Untersuchungsbereich sorgfältig abgesichert wird. Dabei werden interne Ermittler oft auf vertrauenswürdige Unterstützung beispielsweise vom Werk- oder Objektschutz zurückgreifen. Da es sowieso nicht ratsam ist, allein und ohne Zeugen am Ort des Geschehens aufzutauchen, sollte eigentlich eine zweite Person für Sicherungszwecke verfügbar sein. Zu diesem Zeitpunkt ist oft noch nicht klar, ob der Täter eventuell von innen kommt. Möchten die Mitglieder des Expertenteams hier eventuellen Manipulationen vorbeugen, sind entsprechende Vorkehrungen zu treffen, damit Innentäter nicht ihre Spuren verwischen können. In dieser Phase wird durch geeignete Methoden der Grundstein dafür gelegt, dass die gesammelten Informationen in einer eventuell späteren juristischen Würdigung ihre Beweiskraft nicht verlieren. Auch wenn in dieser sehr frühen Ermittlungsphase oft noch nicht richtig klar ist, ob eine juristische Klärung angestrebt wird, sollte trotzdem das Beweismaterial so gesichert werden, dass es auch vor Gericht verwendet werden kann. Aus diesem Grund müssen alle Tätigkeiten sorgfältig protokolliert werden. Dabei kann durchaus auch von Papier und Bleistift Gebrauch gemacht werden. Wichtig ist dabei nur, dass die im Protokoll festgehaltenen Informationen genau sind und der Wahrheit entsprechen. Die gesammelten Daten müssen auch frühzeitig vor versehentlicher oder gar beabsichtigter

Manipulation geschützt werden. Von entsprechenden Hash-Verfahren und dem Vier-Augen-Prinzip ist daher ausgiebig Gebrauch zu machen.

Die Analyse-Phase

In der Analyse-Phase werden die Spuren sorgfältig analysiert und die Ergebnisse objektiv bewertet. Die Schlüsse müssen kritisch hinterfragt werden, um Lücken in der Argumentationskette selbstständig und sicher zu identifizieren.

Die Present-Phase

Während die Secure- und Analyse-Phasen hinsichtlich Detaillierungsgrad und Methode oft unabhängig von der konkreten Fragestellung des Sicherheitsvorfalls sind, sind die Tätigkeiten in der Present-Phase davon abhängig, wer in welcher Form von den Ermittlungsergebnissen überzeugt werden muss. Schlussendlich muss das Ergebnis Personen überzeugen, die während der gesamten Ermittlung nicht anwesend waren und vielleicht auch nicht den technischen Sachverstand aufbringen, alle Details zu verstehen. Dies bedeutet, dass alle Erkenntnisse schlüssig und auch für technische Laien nachvollziehbar dokumentiert und dann überzeugend zielgruppenorientiert präsentiert werden müssen. Die Ergebnisse einer forensischen Untersuchung müssen typischerweise Entscheidungsträgern innerhalb der eigenen Institution, aber durchaus auch externen Entscheidungsträgern und Strafverfolgungsbehörden präsentiert werden.

4.5 Welche Erkenntnisse kann man gewinnen?

Unvoreingenommen den »Tatort« besichtigen

Es hat durchaus Vorteile, den »Tatort« des Geschehens aufzusuchen, ohne eine konkrete Vorstellung davon zu haben, was man dort genau finden wird. Diese Unvoreingenommenheit bei der Analyse eines Sicherheitsproblems sollte immer angestrebt werden. Die Antwort »derzeit unbekannt« hat in manchen Situationen durchaus ihre Berechtigung und kann gerade am Anfang einer Ermittlung den Blick für die nicht offensichtlichen Spuren freihalten. Antworten, die zu schnell und ohne sorgfältige Überprüfung gefunden werden, könnten den echten und wichtigeren Beweis eventuell »vergiften«. Es kommt auch immer wieder mal vor, dass ein Angreifer absichtlich falsche Spuren hinterlässt, um die Ermittler auf eine falsche Fährte zu locken (auch Trugspur genannt). Diese falschen Spuren können z.B. aus falschen IP-Adressen oder Logdatei-Einträgen bestehen.

Grundsätzlich können während dieser Phase der Ermittlung mehrere Tätigkeiten identifiziert werden: Einbruchsanalyse, Schadensfeststellung, Analyse der Angriffstools, Logdatei-Analyse und Suche nach weiteren Spuren. Jeder dieser Schritte ist durch wesentliche Fragestellungen gekennzeichnet und kann für sich allein betrachtet auch Gegenstand einer Einzelfalluntersuchung sein.

Wer hatte Zugang?

Einbruchsanalyse

Um das Ausmaß des Vorfalls und der möglichen Schäden einzuschätzen, ist es wichtig, Hinweise zum möglichen Täter zu erhalten. Erste Informationen, ob es sich um einen mit Insiderwissen ausgestatteten Angreifer oder einen Externen handelt, sind gerade für die weitere Ermittlung von wesentlichem Interesse.

Was hat der Angreifer auf dem System gemacht?

Die Antwort auf diese Frage hat direkte Auswirkung auf die weiteren Ermittlungstätigkeiten. Zudem bestimmt sie die Wahl der Gegenmaßnahmen. Wurden Daten eingesehen, zerstört oder modifiziert? Welche? Wurde Software installiert, die weitere Angriffe vorbereitet oder eine Hintertür für weitere Angreifer öffnet? Wenn die Homepage eines WWW-Servers verändert wurde, ist es von Interesse, ob der Angreifer dort bestimmte Informationen hinterlassen hat. Dies sind zum Beispiel die Bezeichnung der eigenen Gruppe oder der eigene Nickname. Oft finden sich Grüße an befreundete Hacker oder Gruppen (sog. Greetz) auf veränderten Homepages. In einigen Fällen ist es möglich, hier Zusammenhänge zu erkennen, die schlussendlich zur Identifikation des Täters führen.

Wann fand der Vorfall statt?

Der genaue Zeitpunkt oder die mögliche Zeitspanne, während der der Einbruch stattgefunden hat, dient der Korrelation weiterer Daten von anderen Systemen oder Netzkomponenten. Gerade wenn für die weitere Ermittlung Kontakt zu anderen Systemeigentümern oder Internet-Service-Providern nötig ist, muss Klarheit über den Angriffszeitpunkt bestehen. Aus diesen Informationen lässt sich auch ableiten, ab wann der Angreifer die Möglichkeit hatte, weitere Systeme zu kompromittieren oder Daten zu verändern.

Welche weiteren Systeme sind noch betroffen?

Ein wesentliches Ergebnis der Ermittlung ist die Klarheit über das Ausmaß des Angriffs. Für die Einschätzung des Schadens, aber auch bereits für die Planung der Recovery-Maßnahmen ist es wichtig zu wissen, welche Server und Netze noch betroffen waren. Wird festgestellt, dass der Einbruch auf einem Webserver nur dem Zweck diente, interne Systeme anzugreifen, wird natürlich die Suche auch auf diese Server ausgeweitet. Aus Ermittlungssicht kann eine erhöhte Anzahl kompromittierter Server mitunter auch eine erhöhte Anzahl von Spuren und Beweisen bedeuten.

Warum ist gerade dieses Netz oder System angegriffen worden?

Zum besseren Verständnis der Motive des Angreifers sollte man sich auch darüber Gedanken machen, warum gerade dieses System Opfer eines Systemeinbruchs wurde. Hat der Angreifer diesen Server gezielt ausgewählt, oder ist er nur zufällig bei einem großflächigen Portscan auf diesen Server gestoßen? Handelt es sich um ein Gateway-System, liegt die Vermutung nahe, dass jemand Zugang zu einem dahinter liegenden Netz erlangen wollte.

Wie konnte der Angreifer Zugriff erlangen?

Die Technik, die der Eindringling für den Angriff auf das System verwendete, ist für die Ermittlung genauso interessant wie die eingesetzten Tools. Bestimmte Angriffsmethoden ähneln sich oft und könnten eventuell zu ähnlichen Angriffen führen. Dies könnte auch die infrage kommende Tätergruppe einschränken. Wenn für den Angriff zum Beispiel internes Know-how der betroffenen Organisation benötigt wird, ließe es auf einen Innentäter oder einen internen Mittäter schließen. Die Art und Weise des illegalen Zugriffs auf das System oder das gesamte Netzwerk kann auch Aufschlüsse darüber geben, wieso dieser Angriff überhaupt möglich war und welche Versäumnisse beim Systembetreiber lagen. Aufgrund dieser Erkenntnisse können Administratoren aktiv verhindern, dass ein Angreifer über den gleichen Weg in andere Systeme eindringen kann. Dies setzt allerdings voraus, dass die Systembetreiber aus dem Vorfall lernen und die gleichen Fehler nicht wiederholen.

Ist der Angriff vor Kurzem geschehen? Was macht der Angreifer jetzt?

Wenn der Angriff vor kurzer Zeit geschah oder der Angreifer noch aktiv ist, ist es auch für die bessere Einschätzung von Täter und Motiven interessant zu erfahren, was der Angreifer als Nächstes vorhat. Ist zu erwarten, dass er wiederkommt? Wurde er unterbrochen und könnte womöglich wiederkehren, steht die Entscheidung an, ob man mit dem Aufräumen des Schadens wartet und versucht, den Täter weiter zu beobachten.

Was konnte der Angreifer auf diesem System einsehen?

Schadensfeststellung

Zur genaueren Einschätzung des Schadens ist es sinnvoll zu ermitteln, welche Daten oder Informationen theoretisch vom Angreifer hätten eingesehen werden können. Dies betrifft sowohl die Daten und Informationen des lokalen angegriffenen Servers als auch der benachbarten

Systeme. Ein nicht zu vernachlässigender Punkt ist die Gefahr, dass in den angrenzenden Netzwerksegmenten der Datenverkehr belauscht werden kann. Es finden sich auf angegriffenen Systemen häufig spezielle Sniffer, die Passwörter und andere sensible Informationen automatisiert mitschneiden, die dann für weitere Angriffe verwendet werden könnten. Aus diesem Grunde ist es wichtig – nachdem man sicher ist, dass alle Passwort-Sniffer im Netz gefunden wurden –, alle möglicherweise kompromittierten Passwörter zu ändern.

Was wurde vom Angreifer zurückgelassen?

Analyse der Tools

Aus vielerlei Gründen ist es für die weitere Ermittlung wichtig, die zurückgelassenen Tools und Spuren zu analysieren. Die auf dem gehackten System zurückgelassenen Tools oder Spuren sind für die Einschätzung der Fähigkeiten und der Herkunft des Angreifers oft hilfreich. Wurden eigene Tools oder vorgefertigte Werkzeuge verwendet? Wo wurden diese Werkzeuge bereits gefunden? Wenn das angegriffene System als Zwischenstation zum Angriff eines anderen Servers vorgesehen war, finden sich Hinweise auf die möglichen weiteren Ziele?

Welche Tools wurden verwendet?

Es gilt herauszufinden, mit welchen Tools der Angriff vermutlich durchgeführt wurde. Mit dieser Erkenntnis können eventuell Rückschlüsse auf andere Fälle gezogen werden. Die Analyse der gefundenen Werkzeuge liefert oft auch Hinweise auf die Herkunft oder den Programmierer. Gerade bei der Analyse von Rootkits bzw. trojanisierten Systemdateien kann man Erkenntnisse über die Absichten und das weitere Vorgehen eines Angreifers gewinnen. Wenn zum Beispiel ein bestimmter IP-Adressbereich verborgen werden soll, ist anzunehmen, dass von diesen IP-Adressen weitere Aktionen ausgehen werden. Das Auffinden von unbekannten Angriffswerkzeugen kann für weitere Ermittlungen enorm wichtig sein und helfen, frühzeitig Trends bei der Verwendung besonderer Angriffswerkzeuge oder Methoden zu erkennen. Analysen der gefundenen Binärdaten können mitunter Hinweise auf das für die Übersetzung verwendete Betriebssystem geben. Ein weiteres Hilfsmittel, um die Gefährlichkeit des Angreifers einzuschätzen, ist die Analyse, ob eventuelle Rootkits mit den Standardoptionen betrieben werden oder ob deren Default-Passwörter und -Konfigurationsdateien modifiziert wurden. Dies setzt eine tiefere Kenntnis der verwendeten Tools voraus und ermöglicht es dem Angreifer, länger unerkannt zu bleiben, da Rootkits mit den Standardoptionen schnell gefunden werden können. In diesem Fall hätte man es also eher nicht mit einem Anfänger-Hacker bzw. Script Kiddy zu tun.

Wie wurden diese Tools aufgerufen?

Die Art und Weise, wie die Angriffstools aufgerufen wurden, gibt Hinweise auf die Verwendung von vorgefertigten Skripten. Verfügt man z.B. über IDS- oder sonstige Echtzeit-Mitschnitte des Angriffs, kann man erkennen, ob die einzelnen Befehle per Hand eingetippt wurden (verlangsamte Eingabe, eventuelle Tippfehlerkorrekturen), ob sie zeilenweise in die Kommandozeile einkopiert wurden (größere Abstände zwischen den einzelnen Befehlen, die recht lang und komplex sind und sofort erscheinen) oder geskriptete Tools verwendet wurden (schnelle Übergabe von Befehlen ohne längere Pausen zwischen den einzelnen Zeilen).

In welcher Programmiersprache wurden die Tools geschrieben?

Die verwendete Programmiersprache ist sicherlich nur ein kleiner Anhaltspunkt, kann aber durchaus für die Identifikation eines möglichen Täters hilfreich sein. Es ist außerdem zu erwarten, dass komplexere Programmiersprachen nur von bestimmten Personengruppen verwendet werden. Hat man Zugriff auf den Quellcode, finden sich oft Spuren in Kommentarzeilen, Variablenbezeichnungen, Syntaxfehlern oder »Copyright«-Hinweisen. Perl- und Shell-Skripte sind da oft sehr auskunftsfreudig. Sicherlich vermerkt der Angreifer dort nicht seine private Adresse, aber oft finden sich Hinweise auf häufig besuchte IRC-Channel und dort verwendete Nicknames. Mitunter werden Kommentare in der eigenen Muttersprache verfasst. Dies muss aber nicht bedeuten, dass der Angreifer auch der Autor des Skripts oder des Programms ist.

Haben diese Dateien Ähnlichkeiten mit Dateien, die auf dem System eines Tatverdächtigen gefunden wurden?

Hat man einen Täter in Verdacht und steht dessen PC für eine weitere Analyse zur Verfügung, kann ein Vergleich der dortigen Binärdateien mit den auf dem angegriffenen System gefundenen weitere Erkenntnisse bringen. Das Gleiche gilt natürlich auch für Angriffstools, die auf anderen Systemen gefunden wurden. Enthalten die Binärdateien noch Debug-Code, kann dieser sehr leicht verglichen werden. Auch finden sich hin und wieder Hinweise auf die verwendete Entwicklungsumgebung in den Dateien (Pfadnamen und Compiler- bzw. Bibliotheksversionen).

Welche Events wurden protokolliert?

Konnten Angriffsvorbereitung und Durchführung bzw. die zugrunde liegenden verdächtigen Netzverbindungen

Logdatei-Analyse

protokolliert werden? Gibt es verlässliche Firewall-, Router- oder IDS-Logdatei-Einträge? Wenn nein, warum nicht? Sind diese Systeme selbst kompromittiert worden oder hat der Angreifer einen anderen Weg genommen? Finden sich auf dem angegriffenen System vertrauenswürdige Logdateien? Wurden diese vielleicht auf ein anderes System exportiert und sind dann eventuell nicht kompromittiert worden? Existieren History-Daten auf dem System, die nicht durch den Angreifer gelöscht oder modifiziert wurden? Sind nicht kompromittierte Protokolldaten von Dateiintegritäts-Checkern (z.B. Tripwire oder AIDE) vorhanden?

Was wird durch die Protokolldaten enthüllt?

Kann anhand der Protokolldaten nachvollzogen werden, welcher Angriff durchgeführt wurde und welche Schwachstelle zu diesem Angriff geführt hat? Kann man aus den Protokolldaten zuverlässig entnehmen, von welcher IP-Adresse aus der Angriff durchgeführt wurde? Kann man feststellen, ob die Angreifer vom gehackten System aus weitere Server angegriffen haben? Ist aus dem Angriff ein Muster herauszulesen?

Protokolldaten der Remote-Access-Systeme

Besteht der Verdacht, dass der Angreifer nicht über das Internet oder ein angeschlossenes Partnernetz gekommen ist, sondern aus einer internen Netzstruktur, sollten frühzeitig die Protokolldateien der Remote-Access-Systeme (RAS) gesichert werden. Oft kommt es vor, dass ein Angreifer über einen unzureichend gesicherten RAS-Zugang oder mit von einem Notebook gestohlenen RAS-Login-Daten eindringt. Diese Alternative sollte immer bedacht werden. Leider wird in vielen Organisationen keine sinnvolle Protokollierung der RAS-Events durchgeführt.

Protokolldaten der Zutrittskontrollsysteme

Wird ein Innentäter vermutet oder ist ein lokaler Zugriff für den aufzuklärenden Vorfall nötig, sollte man frühzeitig daran denken, die Daten eventueller Zutrittskontrollsysteme bzw. Videoüberwachungsbänder zu sichern. Erfahrungsgemäß bedarf die Einsicht dieser Daten der Mitsprache weiterer Personen (behördlicher bzw. betrieblicher Datenschutzbeauftragter oder Personal- bzw. Betriebsrat). Auch finden sich diese Daten oft nur im Zugriff des Facility-Managements. Um Zeitverlusten durch eventuelle organisatorische Hürden vorzubeugen, sollte in der Ermittlungsphase frühzeitig geklärt werden, ob und wie man auf diese Zutrittsinformationen zugreifen kann.

Was findet sich auf den Datenträgern?

Weitere Beweissuche

Wenn ein Angreifer auf einem System aktiv war, werden fast immer Spuren auf den Datenträgern des Systems hinterlassen. Aus diesem Grund ist es sehr wichtig, sich den Inhalt der Dateisysteme genau anzuschauen und nach auffälligen Spuren für einen Missbrauch zu suchen. Die zu suchenden Spuren hängen im starken Maße von der konkreten Fragestellung des Sicherheitsvorfalls ab: Wurde das verdächtige System für einen Angriff verwendet, ist es selbst angegriffen oder für andere Straftaten verwendet worden?

Welche Spuren sind durch die verwendeten Applikationen hinterlassen worden?

Nicht jede Anwendung arbeitet spurenlos. Fast jede Applikation hinterlässt auf der Festplatte oder in den bearbeiteten Dokumenten Spuren. Besuchte Websites bzw. heruntergeladene Dateien lassen sich häufig durch die vom WWW-Browser hinterlassenen Datenspuren nachweisen. Ebenso kann es unter Umständen gelingen, ein System mit einer erstellten Datei in Verbindung zu bringen, wenn z.B. Merkmale wie der Systemname oder der gerade angemeldete Username in der Datei zu finden sind. Auch die Existenz von diversen Angriffstools lässt sich in verschiedenen Spuren auf dem lokalen System nachweisen. Ein weiterer Schritt ist die Suche nach Schlüsselwörtern, die im Zusammenhang mit der konkreten Ermittlungsarbeit stehen (IP-Adressen, E-Mail-Adressen oder Dateinamen).

Welche Dateien wurden gelöscht?

Manchmal geht es darum nachzuweisen, ob jemand seine Spuren auf dem System verwischen wollte, indem er bestimmte Dateien gelöscht hat. In diesem Fall müssen alle Hinweise auf diese gelöschten Dateien gesammelt werden. Wenn sich die originalen Werkzeuge nicht mehr auffinden bzw. wiederherstellen lassen, kann man diese vielleicht aus den bereits gelöschten Installationsarchiven extrahieren.

Existieren versteckte Dateien?

Hat ein Angreifer oder Tatverdächtiger versucht, Informationen vor den Ermittlern zu verstecken? Alle bekannten Möglichkeiten der Dateimaskierung sollten bedacht werden. Ob es sich um den ungenutzten Bereich der Festplatte bzw. einzelner Sektoren oder nur um einfache Verschleierungsfunktionen der verwendeten Betriebssysteme handelt, jeder mögliche versteckte Speicherort auf einem Datenträger muss analysiert werden.

Existieren verschlüsselte Dateien?

Verschlüsselung ist durchaus ein kontroverses Thema. Im Sinne des Schutzes von vertraulichen Daten ist eine gute und robuste Verschlüsselung das Mittel der Wahl. Aus digitalforensischer Sicht kann eine gute Verschlüsselung den Zugriff auf Informationen erheblich einschränken. Besteht die Möglichkeit, das Passwort zu bekommen, sollten auch die verschlüsselten Informationen eingesehen werden. Einige Verschlüsselungsverfahren sind aber auch unter bestimmten Rahmenbedingungen zu umgehen. Dies kann beispielsweise ermöglicht werden, wenn das verwendete Verfahren Schwächen aufweist, das verwendete Passwort einem Wörterbuch bzw. Brute-Force-Angriff nicht standhält oder temporäre Dateien außerhalb der verschlüsselten Bereiche zwischengespeichert werden. Kann man vielleicht auch auf verschlüsselte Daten zugreifen, finden sich dort eventuell wertvolle Hinweise. Für den Fortgang der weiteren Ermittlungen kann aber auch der einfache Hinweis, dass bestimmte Daten verschlüsselt sind, von Interesse sein.

Existieren versteckte Partitionen?

Bei der Analyse des Festplattenlayouts sollte man alle vorhandenen Partitionen identifizieren. Die Tatsache, dass unter einem Betriebssystem nur ein »Laufwerk« zu sehen ist, bedeutet noch lange nicht, dass nicht noch andere Betriebssysteme oder Partitionen auf der Festplatte vorhanden sind. Diese sollte man unbedingt in die Untersuchung einbeziehen.

Existieren bekannte Hintertür- oder andere Fernzugriffstools?

Bei der Analyse des Festplatteninhalts sollte man verstärkt nach installierten Rootkits oder anderen trojanisierten Systemprogrammen suchen (siehe auch die Ausführungen in Abschnitt 5.11). Diese könnten eventuell die Frage beantworten, auf welchem Weg die Angreifer auf das System gelangt sind. Finden sich hier typische Muster, hat man einen Anhaltspunkt, wonach man auf den anderen betroffenen oder bisher unbehelligt geglaubten Systemen suchen sollte.

4.6 Wie geht man korrekt mit Beweismitteln um?

Die Grundlage für eine erfolgreiche Ermittlung möglicher Tatverdächtiger oder Tatabläufe ist die Gewinnung von Beweismitteln und deren juristisch einwandfreie Behandlung. Dieses ist besonders hervorzuheben, da es sich bei den üblichen Tatspuren in der Mehrzahl um digitale Spuren handelt, die bei falscher Handhabung an Beweiskraft verlieren oder gar gänzlich unbrauchbar gemacht werden könnten. Erschwerend kommt hinzu, dass ein Teil der spannenden Informationen nur eine kurze Halbwertszeit hat. Diese Flüchtigkeit erfordert ein besonnenes und koordiniertes

Erfassen und Sammeln von Daten in den ersten Minuten der Ermittlung, besonders wenn man auf eine »Smoking Gun«-Umgebung trifft, der Eindringling also vielleicht noch auf dem System aktiv ist oder das System gerade verlassen hat. Es muss jedem Beteiligten klar sein, dass – egal, welchen Schritt man am verdächtigen System durchführt – der Systemstatus auf jeden Fall verändert wird.

4.6.1 Juristische Bewertung der Beweissituation

Die gewonnenen Beweise werden u.U. in einem Gerichtsverfahren (zivil- und/oder strafrechtlich) eingebracht (siehe hierzu Kap. 10). Die Gerichtsverwertbarkeit dieser Beweise ist davon abhängig, unter welchen Umständen diese Beweise erhoben wurden. In diesem Zusammenhang ist auch die Abhängigkeit des »Sachbeweises« zum »Personalbeweis« zu betrachten.

Sachbeweis

Ein Sachbeweis kann die Festplatte, bestimmte Logdateien, ein Gutachten oder auch ein Fingerabdruck sein. Dieser Beweis wurde durch eine Person erhoben, in das Verfahren eingebracht und wird im Sachzusammenhang auf seine »Beweiskraft« erläutert. Der Sachbeweis allein hat zunächst keine direkte Aussagekraft. Ein Fingerabdruck z.B. an einer Mordwaffe sagt nur aus, dass die Person, deren Abdruck auf der Waffe festgestellt wird, eben diese in der Hand hatte und so mit dem Fingerabdruck »versehen« hat. Dieser Beweis sagt aber nicht aus, dass dieser Fingerabdruck »bei der Tatausführung« auf die Waffe gelangt ist und somit ein Beweis für die Täterschaft ist. Denkbar ist auch, dass der Inhaber des Fingerabdruckes die Waffe vor der Tatausführung auch in der Hand hatte. Der tatsächliche Täter hat vielleicht Handschuhe getragen und keine Fingerabdrücke hinterlassen.

Durch dieses Beispiel wird deutlich, dass der Sachbeweis (z.B. die Logdatei) allein noch keine Aussagekraft hat. Die Beweiskraft wird durch die Person, die den Beweis erhoben hat, und durch die Person, die den Beweis in den Tatzusammenhang stellt und erläutert, erst deutlich. Der Sachbeweis ist somit eng mit dem Personalbeweis verbunden. Das professionelle Erheben des Beweises und die Darstellung der Person im Strafverfahren – auch vor Gericht – ergeben erst die Beweiskraft.

Die Person, die den Beweis beibringt

Hier wird deutlich, dass eine Person, die den Beweis unrichtig darstellt, widerlegbare Behauptungen oder Interpretationen des Beweises angibt, unglaubwürdig werden kann. Das kann dazu führen, dass der betreffende Beweis bis zur Bedeutungslosigkeit an Beweiskraft verliert. Die sachliche Darstellung der Beweiserhebung, der eingesetzten Verfahren und die Erläuterung der Bedeutung z.B. für die Täterschaft wird ein Richter genau prüfen. Die Integrität der Person und ihre Glaubwürdigkeit sind wesentliche Elemente des Beweises. Ein sachliches, fundiertes Gutachten kann durch eine unglaubwürdige Darstellung, bei der z.B. Vermutungen als

Fakt dargestellt werden, vom Richter als nicht verwertbar zurückgewiesen werden. Der Richter wird dieses Gutachten dann nicht zur Rechtsfindung heranziehen.

Gute Dokumentation, keine Vermischung von Fakten und Vermutungen

In Deutschland ist der Richter grundsätzlich in seiner Beweisführung frei. Das heißt, dass er die Glaubwürdigkeit der Person (die den Beweis im Verfahren darstellt) selbst prüfen wird. Seine Entscheidung wird der Richter begründen, aber wenn er der Meinung ist, dass die Person unglaubwürdig ist, wird der Beweis nicht oder in seiner Aussagekraft eingeschränkt zur Urteilsfindung herangezogen. Daher ist die Person, die den Sachbeweis einbringt, genauso bedeutend wie der Beweis an sich. Eine gute Dokumentation – wie in den folgenden Kapiteln beschrieben – hilft demjenigen, der sich als Zeuge vor Gericht befindet, seine Tätigkeiten bei der Beweiserhebung sicher darzustellen. Dabei sollten die aufgefundenen Tatsachen vor Gericht ganz strikt von den eigenen Bewertungen getrennt werden. Man muss sich immer vor Augen halten, dass es hier um Zahlen, Daten und Fakten gehen muss. Probleme können aber immer dann entstehen, wenn bei den beteiligten Personen aufgrund eines unterschiedlichen Wissensstandes kein Verständnis für technische Zusammenhänge vorhanden ist. Dies macht es umso erforderlicher, dass die darzulegenden Fakten einfach, nachvollziehbar und verständlich präsentiert werden. Interpretationen müssen unbedingt als solche dargestellt werden. Oft werden in solchen Momenten vor Gericht Tatsachen und Annahmen vermischt. Hier ist dringend zu unterscheiden.

Beziehung zwischen Zeuge und Geschädigtem

Ein weiterer Aspekt ist die persönliche Beziehung zum oder die Abhängigkeit des Zeugen vom Geschädigten und eventuell vom Täter bzw. Angeklagten. Grundsätzlich ist eine strukturelle Unabhängigkeit von Vorteil, da dann keine Motivlage im Sinne der Geschädigten oder des Täters vorliegt.

Es liegt auf der Hand, dass die Beweisspuren durch möglichst unabhängige Personen erhoben werden sollten. Diese Unabhängigkeit ist bei einem Ermittlungsbeamten per se gegeben. Es ist aber auch möglich, auf externe Spezialisten zurückzugreifen oder in größeren Organisationen eigenes Personal aufzubauen.

4.6.2 Datenschutz

Wenn man sich mit der Erfassung und Auswertung von protokollierten Daten auf IT-Systemen beschäftigt, kommt man zwangsläufig auf Fragen, die sich im weiten Feld des Datenschutzes bewegen. Die Rechtsnormen des Datenschutzes kommen auch zur Anwendung, wenn Festplatten und Mailboxen ausgewertet werden sollen, die personenbezogene Daten enthalten könnten. Durch die Novellierung des Bundesdatenschutzgesetzes (BDSG), die sich mit dem Arbeitnehmerdatenschutz

beschäftigen, wurden die Hürden für eine Sicherstellung und Auswertung von personenbezogenen Daten nochmals angehoben.

Datenschutzgrundsätze

Die Grundlage des Datenschutzes liegt im Recht auf informationelle Selbstbestimmung, das sich u.a. aus Artikel 2 Abs. 1 des Grundgesetzes ergibt. Paragraf 3a des BDSG gibt die Grundprinzipien des Datenschutzes vor:

- *Datenvermeidung*

  Weitestgehender Verzicht auf Verarbeitung personenbezogener Daten

- *Datensparsamkeit*

  Speicherung von möglichst wenig personenbezogenen Daten

- *Systemdatenschutz als Gesamtziel*

  Datenschutz wird bereits bei der Entwicklung von neuen Systemen berücksichtigt.

- *Anonymisierung*

  Personenbezogene Daten werden durch gesonderte Speicherung der Identifikationsmerkmale verändert und dadurch verfremdet.

- *Pseudonymisierung*

  Identifikationsmerkmale werden durch ein Pseudonym ersetzt. Die Zuordnung zur eigentlichen Person ist nur durch spezielle Zuordnungsregelungen möglich.

§ 31 Bundesdatenschutzgesetz

Gemäß § 31 BDSG (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses) dürfen Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes der Datenverarbeitungsanlage gespeichert werden, nur für diese Zwecke verwendet werden. Unter diese Daten fallen u.a.

- Daten bzgl. Zugangskontrolle und Zugriffskontrolle,
- Netzwerk- und Verkehrsinformationen wie IP-Adressen oder Caller-IDs sowie
- Protokolldaten wie Anmelde- und Abmeldezeiten von Benutzern.

Normalerweise ist die Kontrolle des Datenschutzes und der Datensicherheit und in diesem Sinne auch die Auswertung der Protokolldaten die originäre Aufgabe des betrieblichen bzw. behördlichen Datenschutzbeauftragten.

Datenschutz bei der Ermittlung

Im Vorfeld (also bei der Entwicklung von Incident-Response-Strategien) sollten daher einige Aspekte des Datenschutzes berücksichtigt werden:

- Der Datenschutzbeauftragte und der Betriebs- bzw. Personalrat sollten in die Erstellung eines Konzeptes für die Sicherheitsvorfallbehandlung einbezogen werden. Besonders den Maßnahmen zur ersten Sicherung der flüchtigen Daten sollten die angesprochenen Personengruppen zustimmen.
- Sollte eine Auswertung von Protokolldaten mit möglicherweise personenbezogenen Daten stattfinden müssen, sollte der Datenschutzbeauftragte hiervon informiert werden und dieser Auswertung beiwohnen. Ist Gefahr im Verzug, sollte dies auch durch den Leiter der Revision oder den IT-Leiter wahrgenommen werden. Dies ist unbedingt im Vorfeld in Absprache mit dem Datenschutzbeauftragten zu klären. Neben ermittlungstechnischen Erwägungen ist auch aus Datenschutzgesichtspunkten darauf zu achten, dass das Vier-Augen-Prinzip gewahrt bleibt!
- Im Rahmen eines grundsätzlichen Monitoringkonzeptes sollte bestimmt werden, welche Daten zu welchem Zweck protokolliert werden. Hier ist festzulegen, dass die Aufzeichnung personenbezogener Daten ausschließlich der Gewährleistung eines ordnungsgemäßen und sicheren IT-Betriebs dient. Eine Aufzeichnung von Daten erfolgt nur in dem Umfang, wie es für die Erkennung von Sicherheitsverstößen und deren eventueller Rückverfolgung erforderlich ist. Es ist dort ebenfalls zu definieren, dass personenbezogene Daten zu keinem anderen Zweck erfasst, gespeichert oder ausgewertet werden.
- Alle Personen, die mit der Protokollierung und der genehmigten Auswertung beschäftigt sind, sollten im Rahmen einer Betriebsvereinbarung oder eines Zusatzes zum Leistungs-, Arbeits- bzw. Werkvertrag auf das Datenschutzgesetz verpflichtet werden.
- Es muss festgelegt werden, dass die aufgezeichneten Daten, die eine Zuordnung der protokollierten Events zu einer Person ermöglichen (IP-Adressen, Dial-in-Daten, Useraccounts etc.), ohne ausdrückliche Genehmigung eines Entscheidungsträgers nicht an Dritte weitergegeben werden dürfen.

Ausnahmen für Behörden

Grundsätzlich gilt, dass der Datenschutz bei einer Ermittlung nicht außer Kraft gesetzt ist. Allerdings geben die Gesetze den Behörden (und nur diesen) die Ermächtigung, auch Informationen zu sammeln, zu denen sie wegen des Datenschutzes eigentlich keinen Zugang hätten. Datenschutz soll in diesem Zusammenhang kein Tatenschutz (oder Täterschutz) sein. Daher gibt es den Grundsatz im Datenschutzrecht, dass eine Datenübermittlung stattfinden darf, denn die einschlägigen Gesetze zur Strafverfolgung ermächtigen die betreffenden Behörden dazu.

Das Recht auf informationelle Selbstbestimmung der Personen tritt dann unter Abwägung aller rechtlichen Bedingungen in solchen Fällen hinter den Strafverfolgungsanspruch des Staates zurück. Dabei ist in jedem einzelnen Fall eine Entscheidung darüber zu fällen, ob neben den betreffenden Normen und Tatbeständen auch die Verhältnismäßigkeit der Mittel gegeben ist. Die Auskunftspflicht über die Daten

wird dann durch die Zeugeneigenschaft des Dateninhabers bewirkt. Wenn also der Inhaber der Daten als Zeuge vor Gericht geladen ist, muss er Auskunft über diese Daten geben.

4.6.3 Welche Daten können erfasst werden?

Grundsätzlich lassen sich einige empfindliche Datentypen, die für die Ermittlung von Interesse sind, auf einem IT-System finden:

- *Flüchtige Daten*

  Informationen, die beim geordneten Shutdown oder Ausschalten verloren gehen (Inhalt von Cache und Hauptspeicher, Status der Netzverbindungen, laufende Prozesse etc.)

- *Fragile Daten*

  Informationen, die zwar auf der Festplatte gespeichert sind, aber deren Zustand sich beim Zugriff ändern kann (siehe auch die Ausführungen zu Zeitstempeln in Abschnitt 5.3)

- *Temporär zugreifbare Daten*

  Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z.B. während der Laufzeit einer Anwendung

»Sterile« Datenträger verwenden

Für die Speicherung der Beweise sollten unbedingt »sterile« Datenträger verwendet werden. Diese müssen frei von Viren sein. Idealerweise sollten die Datenträger vor der Verwendung zuverlässig formatiert und von allen vorherigen Datenspuren bereinigt worden sein. Dies sollte vor dem Einsatz überprüft werden. Der Vollständigkeit halber sollten die Werkzeuge und Methoden zur Beweisermittlung und -sicherung vorher erprobt worden sein. Sinnvollerweise – auch für die spätere juristische Würdigung – sollten allgemein anerkannte Verfahren und Werkzeuge zum Einsatz kommen.

4.6.4 Bewertung der Beweisspuren

Während der Analyse-Phase werden die in der Secure-Phase erfassten Daten dahin gehend untersucht, ob sich darin Beweisspuren oder Teile davon befinden, um den fraglichen Sachverhalt aufzukären. Dabei lassen sich im Grunde genommen grob drei Gruppen von Beweisspuren unterscheiden:

- Beweisspuren, die eine bestimmte Theorie untermauern,
- Beweisspuren, die gegen eine bestimmte Theorie sprechen, und

- Beweisspuren, die keine bestimmte Theorie unterstützen oder wiederlegen, sondern lediglich zeigen, dass das System verändert wurde, um Informationen oder Spuren zu verbergen.

Bei der Bewertung der Analyseergebnisse sollte man sich immer darüber im Klaren sein, zu welcher Gruppe die gefundene Information eigentlich gehört und was diese letztendlich aussagen.

4.6.5 Durchgeführte Aktionen dokumentieren

Alle während der Ermittlung durchgeführten Aktionen müssen dokumentiert werden. Es ist sinnvoll, sich im Vorfeld ein eigenes Dokumentationsformat zu definieren und entsprechende Formulare bereitzuhalten. Wichtig in diesem Zusammenhang ist auch, dass die Dokumentation für Dritte verständlich ist und eine unberechtigte Veränderung verhindert wird. Diese Dokumentation kann die Glaubwürdigkeit der Ermittlung, die zu Belastungsmaterial geführt hat, untermauern.

Prüfsummen bei elektronischer Dokumentation

Die verwendete Dokumentationstechnik muss nicht zwingend elektronisch sein – erleichtert aber in elektronischer Form die Weiterverarbeitung. Wird elektronisch dokumentiert, sollte auf jeden Fall mit Prüfsummen gearbeitet werden, damit eine unberechtigte Modifikation erkannt werden kann.

Jede Aktion berücksichtigen

Neben dem allgemeinen Grund für die Untersuchung sollte – wie in Tabelle 4–1 beispielhaft gezeigt – auch für jede einzelne Aktion festgehalten werden, warum dieser Schritt durchgeführt wurde und welche Erkenntnis man sich davon erhofft. Zur besseren Bewertung der gefundenen Spuren ist es wichtig, die aktuelle Umgebung (auch die physische Umgebung) so genau wie möglich zu beschreiben. Hierbei ist auf eine große Detailtreue zu achten.

Verdächtige Dateien sollten auf jeden Fall für eine spätere Analyse kopiert werden. Ebenso sollte man ausgiebig Gebrauch von Screenshots machen. Für das »berührungslose« Festhalten von Bildschirminhalten eignen sich besonders Digitalkameras. Zur besseren Einschätzung der gewonnenen Ergebnisse sollten unbedingt die verwendeten Untersuchungstools mit ihren Versionsnummern festgehalten werden. Mitunter kommt es später zu Diskussionen, ob ein Beweis durch die Verwendung von unpassenden Untersuchungswerkzeugen eventuell verfälscht wurde.

Tab. 4–1 *Beispiel einer Dokumentation der durchgeführten Aktionen*

Lfd. Nr.	Zeit	Befehl	MD5 der Ergebnisdatei	Kommentar
1	16:17:10	netstat –n|nc 10.0.0.1 8000	902afd8e6121e153bbc8cb93013667fd	Anzeige der aktiven Netzverbindungen
2	16:17:30	netstat –an|nc 10.0.0.1 8000	cd6783f8d9a109ffe839912674e2f3cf	Anzeige der offenen Ports
3	16:17:55	nbtstat –c|nc 10.0.0.1 8000	931b672fabcdb2145ae51e2885e9b685	Anzeige des Cache von NBTVerbindungen
[…]				
6	17:30	Sicherstellung des verdächtigen PC im Raum B102	Rechnername/IP-Adresse: lapBER49, 192.168.7.69 Inventarnummer: BER4543.A3 Modell: TA-349 Festplatte (Typ,Größe, S/N): RPA-0802, 80GB, 34567783-A-34546	Anwesende Personen: Herr Müller (Hauptbenutzer des PC) Herr Schulz (Revision, Special Investigation) Herr Meier (IT-Security)

Werden Beweise gesichert (Festplatten, Ausdrucke oder auch Dateien), muss für eine lückenlose Beweiskette gesorgt werden. Es sollte jederzeit nachvollziehbar sein, wer, wann, wie Zugriff auf diese Beweise hatte. Dies ist bei elektronischen Beweisen nicht mehr praktikabel durchführbar, deswegen sollte von jedem elektronischen Beweis eine digitale Prüfsumme erstellt und für den Integritätsnachweis aufbewahrt oder ausgedruckt werden. Nach Möglichkeit sollten Zeugen hinzugezogen werden, die jede durchgeführte Aktion mit einer Unterschrift in der Dokumentation versehen. Dies ist für jeden eingegebenen Befehl etwas unpraktisch, sollte aber wenigstens für alle wesentlichen Feststellungen vorgenommen werden. Jeder gefundene Beweis sollte auf einem Beweiszettel vermerkt werden. Hierzu ist es sinnvoll, eine Beschriftungsnomenklatur zu erstellen, anhand derer die Beweise eindeutig identifiziert werden können. Dieser Zettel kann z.B. auch eine Art Laufzettel für den Beweis darstellen.

4.6.6 Beweise dokumentieren

Beweiszettel

Die gefundenen Beweise sollten so dokumentiert werden, dass bei einer späteren juristischen Ermittlung keine Zweifel an Herkunft, Besitztum und Unversehrtheit bestehen. Aus diesem Grund ist es ratsam, für jedes gefundene bzw. sichergestellte Objekt (Festplatte, PDA, Ausdruck, CD-ROM, Notebook etc.) einen Beweiszettel o.Ä. anzulegen, der den Gegenstand eindeutig identifiziert, die vollständige Anzahl nennt und den Besitzer des Objekts (wenn bestimmbar) dokumentiert. Zusätzlich sollte diesem Beweiszettel eine genaue Beschreibung des Objekts hinzugefügt werden. Gerade wenn mehrere Personen oder Organisationen an der Ermittlung beteiligt sind, sollte man dokumentieren, wer zu welchem Zeitpunkt und aus welchem Grund Zugriff auf Beweisstücke hatte.

Beweiszettel		Fall :
Datum: Uhrzeit	Standort/Fundort	ID:
Ermittler	Zeuge	
Unterschrift Ermittler	Unterschrift Zeuge	

Gegenstand	Anzahl	Beschreibung *(Typ, Hersteller, Farbe, Seriennummer, Identifikationsmerkmale, Inventarnummer, ggfls. Wert etc.)*

Ausgabevermerk

Gegenstand	Dat./Uhrzeit	Herausgabe durch	Empfang durch	Grund
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	
		Name Organisation Unterschrift	Name Organisation Unterschrift	

Schlussübergabe

Durchgeführte Aktionen: *(Rückgabe an Besitzer, Archivierung, Zerstörung etc.)*	*Empfänger, Zeuge* Name Unterschrift Datum
	1)
	2)
	3)
	4)

***Abb. 4–1** Beispiel eines Beweiszettels*

Fundort notieren

Neben dem Beweisstück selbst kommt häufig auch dem Fundort eine besondere Bedeutung zu. Aus diesem

Grund sollte ebenfalls festgehalten werden, wo und unter welchen Umständen das verdächtige Objekt aufgefunden wurde. In manchen Fällen ist dieses Vorgehen scheinbar übertrieben. Die Erfahrung zeigt aber, dass wenn diese Daten nicht frühzeitig erfasst werden, die gefundenen Beweisstücke in einer späteren juristischen Untersuchung an »Glaubwürdigkeit« verlieren könnten. Der Aufwand, der für die Sammlung der Beweismittel betrieben wird, ist auch hier wieder vom Wesen des Sicherheitsvorfalls und der möglichen Tragweite abhängig.

4.6.7 Mögliche Fehler bei der Beweissammlung

Es gibt einige wesentliche Aspekte, die bei der Ermittlung beachtet werden müssen, wenn man an ein »frisch gehacktes« System kommt. Oft befindet man sich dabei in dem Dilemma, dass man einerseits das angegriffene System nicht verändern sollte, aber dennoch vitale Parameter dieses Systems benötigt, gerade wenn die »Colts noch rauchen«.

- *Die Zeitstempel (siehe Abschnitt 5.3) der Dateien auf dem angegriffenen System dürfen nicht verändert werden.*

  Durch das Aufrufen von Systembefehlen auf dem angegriffenen System oder das Ansehen von Konfigurationsdateien ändern sich deren Daten des letzten Dateizugriffs. Zusätzlich ist es fatal, mit Dateien zu arbeiten, die möglicherweise von einem Angreifer modifiziert wurden. Die erste Maßnahme an einem gehackten System sollte daher auch die Dokumentation der aktuellen Uhrzeit sein, damit man einwandfrei erkennen kann, welche Zeitstempel vor bzw. nach der Ermittlung modifiziert wurden.

- *Tools mit grafischer Oberfläche sollten auf dem betroffenen System nicht verwendet werden.*

  Gerade die Verwendung von grafischen Oberflächen bedingt, dass auf dem betroffenen System auf eine Vielzahl von Binärdateien (z.B. Bibliotheken) und Konfigurationsdateien zugegriffen wird. Dadurch ändern sich mit einem Schlag die Zeitstempel des letzten Zugriffs. Zur Verdeutlichung: Beim Start sowohl von Windows als auch des Gnome-Desktops unter Linux werden die Zeitstempel des letzten Zugriffs von mehr als 1.000 Dateien geändert.

- *Verdächtige Prozesse sollten nicht beendet werden.*

  Möchte man herausfinden, ob weitere Angriffstools auf dem System aktiv sind, ist es sinnvoll, eine Liste der laufenden Prozesse auf dem System einzusehen. Es kommt hin und wieder vor, dass beim Beenden eines verdächtigen Prozesses wichtige Spuren beseitigt werden. In der Praxis ist oft auch zu erleben, dass unter Unix von einem Angreifer ein Prozess gestartet und die zugehörige Datei dann gelöscht wurde. Von allen laufenden Prozessen finden sich aber Binärkopien im

Verzeichnis /proc. Wird der Prozess beendet, verschwindet auch diese Kopie, die man für die weitere Ermittlung gut hätte verwenden können. Weiterhin finden sich in den von einem verdächtigen Prozess benutzten Speicherbereichen zusätzliche interessante Informationen.

- *Es sollten keine unprotokollierten Kommandos ausgeführt werden.*

  Wurden Systembefehle oder Kommandos aufgerufen, die sich in keinem Protokoll finden, kann es zu Lücken in der Beweiskette kommen. Dies betrifft auch die Ausgabe der aufgerufenen Kommandos.

- *Es dürfen keine vertrauensunwürdigen Programme bzw. System-tools verwendet werden.*

  War ein Angreifer auf einem System mit Administratorrechten angemeldet, ist zu vermuten, dass er Hintertüren eingebaut oder Systemdateien ausgetauscht hat (siehe Abschnitt 5.11). Ein Ermittler sollte sich unter keinen Umständen auf die Ausgaben der Systemtools verlassen, sondern eigene »saubere« Systemkommandos aus vertrauenswürdiger Quelle verwenden.

- *Security Patches oder Updates nur dann installieren, wenn das Response-Team dies empfiehlt.*

  Möchte man herausfinden, welche Sicherheits- oder Konfigurationslücke zu dem Sicherheitsvorfall geführt hat, ist es sinnvoll, diese Lücke zumindest ein kurzes Zeitfenster lang offen zu lassen. Dieses ist natürlich immer im Einzelfall abzuwägen, da dadurch eventuell zusätzlicher Schaden entstehen könnte. Man kann allerdings auch nachvollziehen, dass ein schockierter Administrator schnell einen Security-Patch einspielt oder eine Firewall-Regel aktiviert, damit ihm kein Fehlverhalten nachgewiesen werden kann. Hier sollte verantwortungsbewusst mit den Mitarbeitern umgegangen werden. Die Erfahrung zeigt im Übrigen nicht nur hier, dass sich ein angenehmes Betriebsklima und eine gute Unternehmenskultur positiv auswirken können.

- *Software nur dann installieren oder deinstallieren, wenn das Response-Team dies empfiehlt.*

  Durch das übereilte Installieren bzw. Deinstallieren von Software auf dem angegriffenen System können wichtige Beweise verloren gehen. Forensik-Tools, die erst auf dem zu untersuchenden System installiert werden müssen, sollten nicht ernsthaft in Erwägung gezogen werden.

- *Protokolle sollten nicht auf die zu untersuchende Platte geschrieben werden.*

  Wenn die verwendeten Programme ihre Protokolldateien auf das gleiche Dateisystem schreiben, können möglicherweise wichtige Beweise zerstört werden, z.B. Daten im File Slack oder in unallozierten Dateisystembereichen.

Stecker ziehen?

- *Ein ordnungsgemäßer Shutdown könnte Beweise vernichten.*

  Die Entscheidung, ob man ein System ordnungsgemäß herunterfährt oder ob es einfach durch das sprichwörtliche Steckerziehen vom Stromnetz genommen wird[1], hängt von vielen Faktoren ab. Beim ordnungsgemäßen Shutdown werden wieder sehr viele Dateien »angefasst«, dadurch werden die Zeitstempel des letzten Zugriffs verändert. Ist das System so konfiguriert, dass der Swap-Bereich beim Shutdown gelöscht wird, können auch hier wertvolle Informationen, die aus dem Hauptspeicher stammen, vernichtet werden. Nicht alle Dateisysteme verkraften ein hartes Herunterfahren, allerdings ist nicht zu erwarten, dass man mit dem Server ohne Neuinstallation weiterarbeiten wird. Ist das System ausgeschaltet worden, findet sich ein kompletter Status der laufenden Umgebung auf den Dateisystemen, allerdings lassen sich die flüchtigen Informationen kaum mehr hervorholen. Die letztendliche Entscheidung muss immer im Kontext des konkreten Falls getroffen werde. Wie bereits festgestellt: Der Status des Systems wird in jedem Fall verändert!

4.7 Flüchtige Daten sichern: Sofort speichern

Wird man zu einem System gerufen, das im Verdacht steht, gehackt worden zu sein, ist es wichtig, innerhalb kürzester Zeit so viele vitale Informationen wie möglich zu sammeln, ohne dabei überall seine eigenen »Fingerabdrücke« zu hinterlassen. Es handelt sich hierbei um wichtige Statusdaten, die sowohl nach einem Shutdown als auch nach einem harten Ausschalten des Systems nicht mehr verfügbar sind.

Keine Systembefehle verwenden!

Es sei auch an dieser Stelle nochmals darauf hingewiesen, dass man für die Sammlung dieser flüchtigen Informationen unter keinen Umständen die Systembefehle verwenden darf. Der Grund liegt zum einen darin, dass es sich um trojanisierte Programme handeln kann, die entweder bestimmte Informationen verbergen oder auch Schadfunktionen aktivieren können. Die Verwendung der lokalen Kommandos würde deren Zeitstempel des letzten Aufrufs verändern. Aus diesem Grund sollte mit eigenen sicheren und aus vertrauenswürdiger Quelle stammenden Dateien gearbeitet werden.

Die Protokolldateien sollten entweder auf eine Diskette, in einer RAM-Disk oder über das Netz geschrieben werden. Hier eignet sich auch der Einsatz von Skripten oder Batch-Dateien, die die benötigten Informationen sehr schnell sammeln können.

Unabhängig davon, welche der in Abschnitt 7.1.1 und 7.2.1 vorgestellten Tools und Verfahren Sie zum Sammeln der benötigten Daten verwenden, sollten grundsätzlich folgende Informationen gesammelt werden:

- Systemdatum und -uhrzeit (mit Abweichung von einer Referenzzeit)
- Liste der aktiven Prozesse

- Liste der geöffneten Sockets
- Liste der Anwendungen, die auf geöffneten Sockets lauschen
- Liste der User, die gerade angemeldet sind
- Liste der Systeme, die gerade eine Netzverbindung haben oder vor Kurzem eine hatten

Sind diese Daten erfasst, kann man sich auf die Suche nach weiteren verdächtigen Spuren machen.

Grundsätzlich wird gesucht nach

- Timestamps des gehackten Systems,
- trojanisierten Systemprogrammen,
- versteckten Dateien und Verzeichnissen,
- verdächtigen Dateien oder Sockets und
- verdächtigen Prozessen.

Häufig genügt ein einzelner Ansatzpunkt, um die richtige Spur zu finden!

Aktuelle Uhrzeit

Damit alle eingegebenen Befehle einem Startzeitpunkt zugeordnet werden können, sollte unbedingt die lokale Uhrzeit des Systems erfasst werden. Alle Aktionen, die ab diesem Zeitpunkt erfolgen, sollten einwandfrei der Ermittlungstätigkeit zuordenbar sein.

Cache-Inhalt

Der Inhalt von Cache- und Auslagerungsdateien ist für die Analyse von laufenden Programmen oder abgesetzten Befehlen von Interesse. Soweit in einer laufenden Umgebung Zugang zu diesen möglich ist, sollten diese erfasst werden. Der Umfang übersteigt allerdings den Speicherplatz, den eine normale Diskette bietet.

Speicherinhalte

Der Inhalt des Hauptspeichers sollte komplett und auch im Prozesskontext erfasst werden. Für die einfachere Auswertung sollte der einer Prozess-ID zugeordnete Hauptspeicherinhalt jeweils separat erfasst werden. Auch diese Informationen passen nicht auf eine Diskette.

Status der Netzverbindung

Wesentliche Anhaltspunkte über eventuell aktive Hintertürprogramme finden sich auch in der Auflistung der offenen Netzwerkports. Zusätzlich lässt sich auch erkennen, ob Verbindungen gerade aufgebaut oder im Abbauprozess sind. Finden sich z.B. sehr viele Verbindungsaufbauanfragen, ist davon auszugehen, dass dieses System für einen Distributed-Denial-of-Service-Angriff oder einen Portscan verwendet wurde. Einige Betriebssysteme führen eine Statistik über die Anzahl der erfolgreichen oder erfolglosen Verbindungsaufbauversuche. Diese kann mit einem Befehl ausgelesen werden. Weiterhin ist es natürlich von Interesse, welche Applikation bzw. welcher Service den Port geöffnet hat.

Status der laufenden Prozesse

Eine Liste der aktuell laufenden Prozesse sollte gesichert werden. Zusätzlich sollten weitere Informationen (Umgebungsvariablen, Übergabeparameter, geladene Bibliotheken, offene Dateideskriptoren etc.) gespeichert werden.

Inhalt der Speichermedien

Finden sich in dem System Disketten oder Wechselmedien, sollten diese sichergestellt werden.

Beispiele zum Sammeln der gerade erwähnten Informationen können den folgenden Kapiteln 6 und 7 entnommen werden.

Inhalt des Hauptspeichers

In zunehmendem Maße ist es wichtig, auch den Hauptspeicher (RAM) des verdächtigen Systems zu sichern. Hierbei geht es nicht nur darum, den gesamten Speicherinhalt als eine große Datei zu sichern, sondern auch stukturelle Informationen. Hierzu gehören beispielsweise die Informationen, welcher Prozess welche Bibliotheken geladen hat bzw. bestimmte Speicherbereiche belegt. Unter gewissen Umständen lassen sich diese Informationen auch im Nachhinein aus einem Hauptspeicherdump herauslesen. Wenn man auf Nummer sicher gehen will, sollten die Daten sowohl stukturiert als auch als Komplettdump sichergestellt werden.

4.8 Speichermedien sichern: Forensische Duplikation

Ein Standardverfahren

Die forensische Duplikation von sichergestellten Speichermedien hat sich quasi zu einem

Standardvorgang bei der Ermittlung im Umfeld der Computerkriminalität entwickelt. Ein forensisches Duplikat ist letztendlich lediglich ein Image eines Datenträgers, das bitweise als eine 1:1-Kopie sicher erzeugt wurde. Dabei wird, unabhängig von den logischen Laufwerkszuordnungen, der gesamte physische Datenträgerinhalt übertragen.

Grundsätzlich können mehrere Verfahren zum Einsatz kommen, wobei die letztendlich gewählte Variante auch von den lokalen Gegebenheiten am Einsatzort abhängt:

- Die verdächtige Festplatte wird aus dem gehackten System entfernt und dann an das Analysesystem des Ermittlers angeschlossen.
- An das gehackte System wird eine zusätzliche saubere Festplatte des Ermittlers angeschlossen.
- Die kopierten Daten werden über ein (geschütztes) Netzwerk auf das Analysesystem des Ermittlers übertragen.

Um das versehentliche Überschreiben der Festplatte zu verhindern, sollten unbedingt zusätzlich sogenannte Writeblocker angeschlossen werden. Diese Geräte verhindern physisch, dass auf den zu sichernden Datenträger schreibend zugegriffen wird. Der Datenträger kann ganz normal auch unter Windows oder Linux sichtbar gemacht werden, ein Schreiben ist aber nicht möglich. Wird ein Writeblocker bei der Image-Erstellung verwendet, kann keine Partei in der juristischen Aufbereitung ein versehentliches Schreiben und damit unsauberes Arbeiten unterstellen. Writeblocker gibt es von verschiedensten Herstellern für USB-, SCSI-, Firewire- oder IDE-Schnittstellen.

Neben den in Abbildung 4–2 gezeigten mobilen Writeblockern gibt es auch stationäre, in Analysesysteme eingebaute Writeblocker, die oft bessere Geschwindigkeiten erzielen.

Abb. 4–2 *Der Writeblocker wird zwischen Analysesystem und zu sichernder Festplatte positioniert (in diesem Bild ist der Writeblocker via USB an das Analysesystem angeschlossen).*

HPA

Bei der Erstellung einer forensischen Duplikation ist darauf zu achten, dass es auf Datenträgern mittlerweile zahlreiche Bereiche gibt, in denen Daten versteckt werden können. So wird beispielsweise die Host Protected Area (HPA) in der Regel vom Festplattenhersteller zum Speichern von Informationen verwendet, die nur mittels ATA-Kommandos zugreifbar sind. Das für die Duplikation verwendete Verfahren und Betriebssystem sollte in der Lage sein, HPA und andere schwer zugreifbare Bereiche zu erkennen und zu sichern. Ein ähnlicher Bereich ist auch der Device Configuration Overlay (DCO).

4.8.1 Wann ist eine forensische Duplikation sinnvoll?

Die Arbeit an einem mittels forensischer Duplikation erzeugten Festplatten-Image bringt enorme Vorteile. Im Gegensatz zu den Tätigkeiten, die bei der Erfassung von flüchtigen Daten an einem Live-System durchgeführt werden müssen, kann sich der Ermittler seinen eigenen Untersuchungspfad legen und muss nicht ständig Gefahr laufen, dass Informationen verschwinden oder zerstört werden könnten. Das forensische Duplikat kann beliebig kopiert werden; die Gefahr von Datenverlust oder -modifikation besteht nicht, da mit Prüfsummenverfahren gearbeitet werden kann. Es können an diesen

Kopien mehrere zeitaufwendige Tätigkeiten gleichzeitig durchgeführt werden, während das Originalsystem vielleicht schon wieder neuinstalliert wird. Auch lässt sich die Arbeit gut über mehrere Personen verteilen, um eventuell unterschiedlich vorhandenes Know-how besser zu bündeln.

Während die Untersuchung am Live-System mit der Arbeit in einer Notaufnahme vergleichbar ist, ähnelt die Arbeit am Festplatten-Image der Arbeit in der Gerichtsmedizin. Es ist wohl unbestritten, dass – diesem Vergleich folgend – im Sektionssaal der Gerichtsmedizin eine gründlichere und stressärmere Arbeit möglich ist als im Schockraum der Notaufnahme.

Die Auswertung von Daten auf einem forensischen Duplikat einer Festplatte kann mitunter sehr zeitaufwendig sein. Die Entscheidung, ob ein solches Duplikat angefertigt werden sollte, hängt im Wesentlichen von der Beantwortung der folgenden Fragen ab:

- Kann es zur straf- oder zivilrechtlichen Ahndung kommen?
- Entsteht durch Produktionsausfall ein hoher Verlust?
- Entsteht durch Zerstörung ein hoher Verlust?
- Müssen Daten als Beweis wiederhergestellt werden?
- Muss der freie Speicherbereich durchsucht werden?

Ist eine der genannten Fragen positiv zu beantworten, ist i.d.R. eine forensische Duplikation der Festplatten des zu untersuchenden Systems sinnvoll.

4.8.2 Geeignete Verfahren

Bewertung der Verfahren

Es gibt eine Vielzahl von Werkzeugen, die den Ermittler bei der Erstellung von forensischen Duplikaten unterstützen. Einige dieser Tools werden in den Kapiteln 6 und 7 näher vorgestellt. Wenn auch die Grundfunktionalität und die zugrunde liegende Technologie keine bahnbrechenden Neuerungen erfahren haben, ist der Anbietermarkt dynamisch. Bei der Auswahl oder Bewertung eines Werkzeugs oder einer bestimmten Technologie sind deswegen wesentliche Anforderungen zu stellen:

- Die Übertragung der Daten muss bitweise erfolgen. Jedes Bit des Untersuchungsmediums muss übertragen werden.
- Lesefehler müssen zuverlässig und robust behandelt werden. Nach mehrfachem Leseversuch muss der fehlerhafte Sektor markiert und mit einem Platzhalter versehen werden.
- Es dürfen keine Änderungen am Originalmedium vorgenommen werden. Der Zugriff darf nur lesend erfolgen.
- Die Anwendung muss nachvollziehbar arbeiten. Alle Aktionen müssen durch einen Dritten die gleichen Ergebnisse liefern. Dies ist gerade für die gerichtliche Verwertung der gewonnenen Erkenntnisse von wesentlicher Bedeutung.

- Das erstellte Image muss durch kryptografische Verfahren (Checksummen oder Hash-Algorithmen) geschützt werden können. Veränderungen am erstellten Image müssen damit zuverlässig und sofort erkannt werden können.

Werden Festplattenkopien angelegt, ist unbedingt sicherzustellen, dass die Zielplatte keine alten Datenreste enthält.

Einige Hersteller von Dupliziersystemen sind dazu übergegangen, nicht mehr das gesamte Festplatten-Image im Rohformat zur Verfügung zu stellen, sondern die für die Analyse wesentlichen Informationen bereits zu extrahieren. Dies hat sicherlich im Sinne einer besseren Performance Vorteile und erspart aufwendige Zwischenschritte. Der Ermittler muss dann aber häufig vor der Duplikation entscheiden, was er analysieren möchte. Die Anwendung von neuen Analysemethoden könnte dann im Nachhinein erschwert werden, da bereits eine »Vorverdichtung« der Daten stattgefunden hat. Zusätzlich bleibt manchmal ein fader Beigeschmack, da nicht immer so genau zu überblicken ist, was gerade mit den Daten passiert. Aus diesem Grunde empfiehlt es sich, ein »echtes« Festplatten-Image zu erstellen und es dann mit diesen erweiterten Tools zu bearbeiten. Die meisten professionellen Werkzeuge erlauben die unproblematische Analyse von bereits erstellten Festplatten-Images. Somit ist die Gefahr des Beweiskraftverlustes ebenfalls abgeschwächt.

Hardwarelösungen

Neben Verfahren, die als reine Softwarelösung fungieren, kann eine forensische Duplikation auch über spezielle externe Geräte durchgeführt werden. Dies hat den Vorteil, dass hier mit größeren Geschwindigkeiten dupliziert werden kann, was gerade die Sicherung von mehreren großen Festplatten erleichtert. Hier gilt aber ebenfalls, dass das erstellte Image nicht modifiziert werden darf. Dies kann aber sehr einfach mittels Prüfsummen kontrolliert werden.

4.9 Was sollte alles sichergestellt werden?

Steht man vor der Aufgabe, einen PC für die Analyse sicherzustellen, sollte erwogen werden, folgende Dinge mitzunehmen:

- Haupteinheit, in der alle maßgeblichen Komponenten enthalten sind (normalerweise reichen die eingebauten Datenträger aus, aber am Anfang kann man dies noch nicht so genau wissen).
- Monitor und Tastatur nur in besonderen Fällen, wenn es sich beispielsweise um Spezialgeräte mit Zusatzfunktionen für die Authentisierung handelt.
- Externe Stromkabel, wenn es sich um Spezialkabel handelt oder diese für die Versorgung von externen Geräten verwendet werden, die auch sichergestellt werden.

- Externe Festplatten, Disketten, DVD, CD, WORM und Backup-Bänder, die sich im näheren Umfeld des verdächtigen Systems befinden.
- Speicherkarten, die sich im näheren Umfeld oder am Tatverdächtigen selbst befinden (für die Durchsuchung der persönlichen Kleidung sollte für private Ermittler die geeignete Rechtsgrundlage vorhanden sein). Besonders ist hier auf USB-Sticks an Schlüsselbunden etc. zu achten.
- Externe Kommunikationssysteme, die für die Identifikation einer Verbindung oder auch deren Missbrauch analysiert werden müssen. Hierzu zählen WLAN-Router, DSL- und analoge Modems, ISDN-Adapter, aber auch WLAN-, ISDN-, Ethernet-PCMCIAKarten.
- Geht es in der aufzuklärenden Fragestellung um die Benutzung von Spezialsoftware, die nur mit Dongles oder besonderen Lizenzmerkmalen verwendet werden kann, sollte der Zugriff auf diese Dongles möglich sein.
- Bei entsprechender Fragestellung sind Digitalkameras sowie MP3-Player und deren Speicherkarten ebenfalls zu analysieren, denn eine Kamera kann nicht nur Grafikdateien speichern, sondern auch als normales Massenspeichermedium verwendet werden.
- Mit zunehmender Bedeutung von Personal Digital Assistents (PDA) und Mobiltelefonen sind auch diese sicherzustellen. Zum einen können sich hier Hinweise auf Kommunikationspartner finden, zum anderen auch gespeicherte Daten analysiert werden.

Bei allen sicherzustellenden Systemen und Komponenten sollte abgewogen werden, ob durch die Komplettsicherstellung nicht hinnehmbare Beeinträchtigungen der Arbeitsfähigkeit entstehen können und dadurch der Schaden eventuell noch größer wird als durch das eigentliche Delikt selbst.

4.10 Erste Schritte an einem System für die Sicherstellung

Unabhängig von der konkreten Fragestellung und dem verwendeten Betriebssystem gibt es ein paar allgemeingültige Schritte bei der Sicherstellung eines verdächtigen Client-PC zu betrachten. Bei Serversystemen kann es zu abweichenden Handlungen kommen. Auf jeden Fall sollte man sich im Vorfeld Gedanken machen, wie bei einer Sicherstellung im eigenen Zuständigkeitsbereich vorzugehen ist.

4.10.1 System läuft nicht (ist ausgeschaltet)

1. Alle fremden Personen vom System und der Stromversorgung entfernen.

2. Umgebung fotografieren bzw. Skizze anfertigen (Standort der Systeme und Monitore etc.)
3. Eventuell aktive Druckjobs zu Ende laufen lassen.
4. Unter keinen Umständen das System einschalten! (Vorsicht bei Notebooks: Sie können sich einschalten, wenn man den Deckel öffnet.)
5. Sicherstellen, dass das System wirklich ausgeschaltet ist (Bildschirmschoner können oft täuschen).
6. Ist das System eventuell im Standby-Modus? Sonst bei Notebooks Akkus entfernen, damit nicht ein Energiesparmodus anspringt und möglicherweise Zeitstempel verändert.
7. Stromkabel am Gerät entfernen.
8. Netzwerkkabel entfernen, damit eine WakeOnLan-Funktion den Rechner nicht wieder hochfahren lässt.
9. Alle sichergestellten Geräte und Objekte müssen eindeutig beschriftet werden (wichtig, wenn die Analyse und Sicherstellung durch unterschiedliche Personen durchgeführt werden).
10. Nähere Umgebung nach Notizen oder Papierunterlagen durchsuchen.
11. Nach Möglichkeit sollte der Anwender nach Besonderheiten des Systems, Passwörtern oder anderen Konfigurationsspezifika befragt werden. Die Antworten sollten genau dokumentiert und bei Bedarf kritisch hinterfragt werden.
12. Dokumentation aller mit der sichergestellten Hardware durchgeführten Tätigkeiten.

4.10.2 System läuft (ist eingeschaltet)

1. Alle fremden Personen vom System und der Stromversorgung entfernen.
2. Umgebung fotografieren bzw. Skizze anfertigen (Standort der Systeme und Monitore etc.)
3. Nach Möglichkeit Anwender nach Besonderheiten des Systems, Passwörtern oder anderen Konfigurationsspezifika befragen. Die Antworten sollten genau dokumentiert und bei Bedarf kritisch hinterfragt werden.
4. Bildschirminhalte festhalten (mit Digitalkamera o.Ä.).
5. Keyboard und Maus nach Möglichkeit nicht sofort berühren. Ist der Bildschirm »blank«, sollte der Ermittlungsleiter befragt werden, ob durch Mausbewegung der Bildschirminhalt hergestellt werden soll. Der genaue Zeitpunkt der »Mausbewegung« sollte notiert werden, da dadurch unter Umständen Zeitstempel verändert werden können.

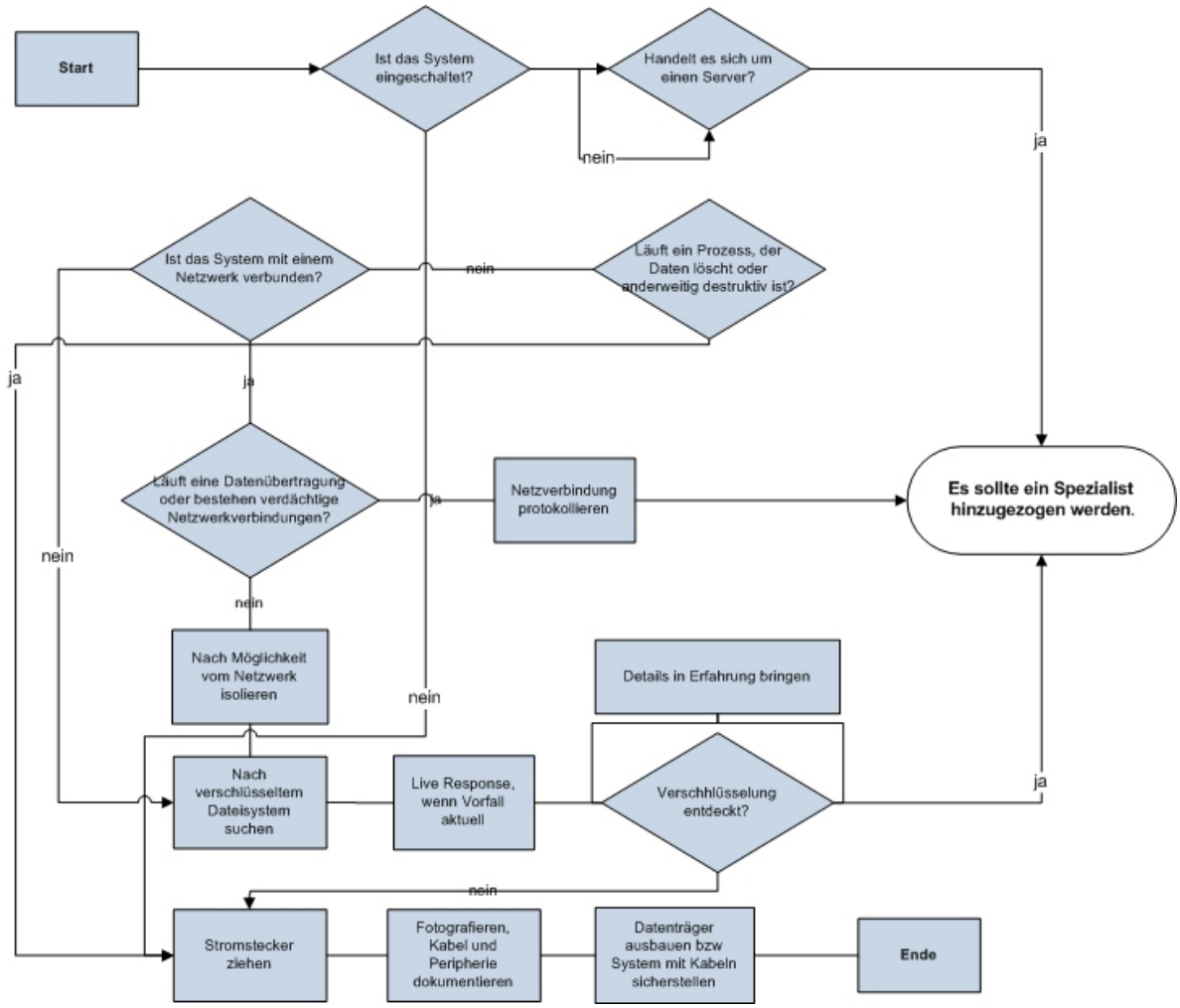
6. Wo möglich/nötig, Durchführung einer Live Response (flüchtige Daten, die nach dem Ausschalten verloren sind, nicht-invasiv sichern). Alle Tätigkeiten sollten mit genauer Uhrzeit protokolliert werden.
7. Alle weiteren Schritte dann wie oben beschrieben ausführen.

Bei anderen Systemen, beispielsweise PDA und Mobiltelefonen, müssen abhängig von der verwendeten Technologie unterschiedliche Methoden angewandt werden (siehe Abschnitt 7.3.3).

4.10.3 Entscheidungsprozesse

Jeder Sicherheitsvorfall ist individuell und kann besondere Entscheidungen erfordern. Zusätzlich zu den in den beiden vorherigen Unterkapiteln aufgeworfenen Fragen lassen sich noch weitere Entscheidungsbäume abfragen, die zu einem groben standardisierten Vorgehen führen. In Anlehnung der Empfehlungen der International Association of Computer Investigative Specialists (IACIS) kann das folgende Ablaufdiagramm als Basis dienen. Hierbei geht es darum, dass in den ersten Stunden nach einem Sicherheitsvorfall oft kein Computer-Forensik-Spezialist in der Nähe ist, der lokale Nicht-Spezialist aber Entscheidungen treffen muss.

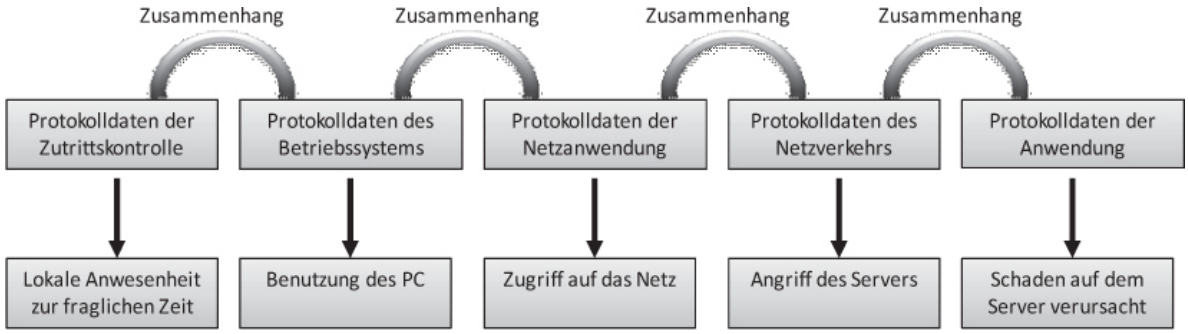
Abb. 4–3 *Beispielhafter Ablauf einer Erstreaktion durch NichtSpezialisten*



4.11 Untersuchungsergebnisse zusammenführen

Es ist sicherlich nicht sehr komplex, die einzelnen Spuren aus den oben beschriebenen Quellen zu sammeln. Hierzu bedarf es guter handwerklicher Fähigkeiten und der Kenntnis der jeweiligen Plattform, einiges wird auch durch komfortable Werkzeuge abgenommen. Die Herausforderung bei jeder Ermittlung besteht aber darin, alle diese Beweise in einen kausalen und auch zeitlichen Zusammenhang zu bringen und entsprechende Schlüsse daraus zu ziehen. Die bei der forensischen Analyse von digitalen Spuren gefundenen Untersuchungsergebnisse müssen mit anderen Ereignissen korreliert, also in Zusammenhang gebracht werden. Die zeitlichen Abläufe müssen plausibel und nachvollziehbar sein. Häufig lassen sich die einzelnen Spuren sehr gut nachweisen und interpretieren. Die Erfahrung zeigt aber, dass gerade der Zusammenhang kritischen Fragen standhalten muss.

Abb. 4–4 *Herstellen der zeitlichen Abhängigkeiten zwischen den einzelnen Tatspuren*



Würdigung des Umfelds

Durch die Herstellung des Zusammenhangs der digitalen Beweise mit »physischen« Beweisen kann ein genaueres Bild vom möglichen Tathergang gezeichnet werden. Eine abschließende Bewertung des gesamten Sachverhalts ohne die Würdigung des weiteren Umfelds ist nur in den seltensten Fällen möglich. Die folgenden Fragen dienen der Erweiterung Ihres Blickfelds bei der Beurteilung von digitalen Spuren:

- War für die Durchführung der strafbaren Handlung ein physischer Zugang zum PC nötig?
- Welche Personen hatten außer dem Verdächtigen noch Zugang zu dem Computer?
- War auf dem PC ein Cronjob oder Scheduler aktiv, der die verdächtige Handlung ohne Anwesenheit des Tatverdächtigen durchführen konnte?
- Besteht eventuell die Möglichkeit, dass die digitalen Spuren durch Fremdeinwirkung Dritter zustande gekommen sein könnten?
- Existieren weitere Beweise, die die Aussagen der digitalen Spuren bestätigen oder diesen widersprechen?
- Über welche Computerkenntnisse verfügen der Tatverdächtige bzw. seine Mittäter wirklich bzw. welche Kenntnisse sind für die Tatdurchführung nötig?
- Ist die Hardware transportabel oder kann der Tatverdächtige seinen Standort durch die Verwendung mehrerer Computer verschleiern?
- Kann ein geschriebener Angriffscode oder ein verräterisches Dokument bzw. eine E-Mail in Verbindung zum Tatverdächtigen gebracht werden (z.B. durch Stil, Vokabular oder bestimmte Redewendungen)?
- Können die gefundenen Spuren über besuchte Webseiten mit dem Sachverhalt in Verbindung gebracht werden?
- Finden sich Hinweise auf E-Mails oder Chat-Rooms bzw. IRCChannels, die eventuelle Mittäter oder Mitwisser identifizieren könnten?

Diese Aufzählung muss im konkreten Einzelfall um weitere Fragestellungen ergänzt werden.

4.12 Häufige Fehler

Nicht nur beim Umgang mit Beweismitteln, sondern auch bei der grundsätzlichen Behandlung von Sicherheitsvorfällen werden oft wesentliche Fehler gemacht, die eine weitere Ermittlung bzw. gerichtliche Verwertung der gewonnenen Beweise erschweren.

Kein Incident-Response-Plan in Vorbereitung

Incident-Response-Pläne helfen nicht unbedingt, den Eintritt eines Schadens zu verhindern. Dies kann nur über flankierende Maßnahmen erreicht werden. Eine gute Vorbereitung ermöglicht es aber, dass jeder Mitarbeiter seine Rolle bei einem Sicherheitsvorfall kennt und entsprechend handelt. Sind gewisse Alarmierungs- bzw. Eskalationsprozeduren ausgearbeitet und ist dokumentiert, welche Schritte einzuleiten sind, können die richtigen Personen frühzeitig informiert und damit die Ermittlungen schnell eingeleitet werden. Es darf nicht vergessen werden, dass ein Notfall (und das kann ein Sicherheitsvorfall durchaus sein) immer eine Ausnahmesituation darstellt und man immer mit Ausnahmereaktionen der Mitarbeiter rechnen muss. Sind gewisse Abläufe für solche Krisensituationen niedergeschrieben, besteht die Chance auf eine saubere und professionelle Abwicklung.

Unterschätzen der Tragweite des Vorfalls

In einigen Fällen kommt es leider oft auch zu einer Fehleinschätzung der Tragweite des Sicherheitsvorfalls. Die Folgen, die ein kleiner Systemeinbruch eventuell für alle angrenzenden Systeme haben könnte, werden dabei übersehen. Dies gilt z.B. auch für die Folgen des Diebstahls eines Außendienst-Notebooks, das für einen Fernzugriff verwendet werden kann. Einbrüche, die oberflächlich betrachtet nur der eigenen Umgebung galten, könnten eine Ausstrahlung auf Systeme Dritter haben. Die Pressemeldung, dass auf einem System der Organisation eingebrochen wurde, ist unangenehm genug für diese Organisation. Welcher Imageschaden aber entsteht, wenn es heißt, dass über einen Angriff auf diese Organisation die Systeme der Partner und Dritter kompromittiert wurden? Der mögliche zivilrechtliche Schadensersatzprozess würde den Verantwortlichen der Organisation, die den Angriff z.B. durch Fahrlässigkeit ermöglicht hat, erhebliche Probleme bereiten.

Keine rechtzeitige Meldung über den Vorfall

Wie die folgenden Kapitel zeigen werden, ist es mitunter möglich, unmittelbar nach einem erfolgten Angriff wesentliche Informationen zu erfassen. Je länger man mit dem Start der Ermittlung wartet, desto mehr Spuren können absichtlich oder zufällig unbrauchbar gemacht werden. Sind die Administratoren nicht ausreichend für die Problematik sensibilisiert, werden sie für das Bemerken von Verdachtsmomenten, dass ein Einbruch stattgefunden hat, mehr Zeit benötigen, als zur Verfügung steht. Die

Entscheidung, Kontakt zu einem externen oder internen Ermittler aufzunehmen, kann zusätzlich dadurch verzögert werden, dass die Entscheidungsträger im Unklaren gelassen werden.

Entscheidungsträger sind nicht oder nur unzureichend informiert

Eine weitere Fehlerquelle, die oft zu Verzögerungen bei der Ermittlung führt, ist die unzureichende Information der Entscheidungsträger. Werden diese frühzeitig einbezogen, ist es mitunter möglich, rechtzeitig Business-Continuity-Maßnahmen einzuleiten und somit den Schaden einzudämmen. Eine frühzeitige Information der richtigen Personen im Unternehmen ermöglicht es auch zu entscheiden, ob Anzeige erstattet wird und wer überhaupt Kontakt zu den Polizeibehörden aufnehmen kann. Hier herrscht in den Unternehmen häufig Unklarheit.

Keine durchgängige Dokumentation der durchgeführten Aktionen

Wenn nicht jede wesentliche Aktion der Beweissicherung so lückenlos wie möglich dokumentiert ist, kann man eventuell zu einem späteren Zeitpunkt nicht mehr nachvollziehen, wie die Ermittler zu ihren Entscheidungen und Einschätzungen gelangten. Der Dokumentation sollte auch zur eigenen Absicherung entnommen werden können, dass man alles unternommen hat, um den bereits entstandenen Schaden zu begrenzen oder weiteren Schaden zu vermeiden.

Digitale Beweise sind unzureichend vor Veränderung geschützt

Sollen die gewonnenen Beweise für eine juristische Verfolgung herangezogen werden, muss sichergestellt werden, dass keine unberechtigten Personen Zugriff auf die entsprechenden Beweismittel hatten. Ebenso dürfen die Beweismittel nicht verändert werden können. Oft wird leichtsinnig mit den erfassten Informationen umgegangen. Dies betrifft besonders elektronische Beweise, da diese oft ohne die nötigen Prüfsummen gespeichert werden. Treten später Zweifel an der Unverfälschtheit eines Beweises auf, können alle darauf basierenden Erkenntnisse oder Schlüsse in Mitleidenschaft gezogen werden. Wie bereits erwähnt, kommt dem Schutz der Beweismittel eine wesentliche Bedeutung zu. Dies ist besonders wichtig, da es sich in der Mehrheit um elektronisch verfälschbare Informationen handelt, deren Integrität zweifelsfrei sein muss. Oft werden diese Informationen ungeschützt auf wiederbeschreibbaren Datenträgern oder gar in »Reichweite« des angegriffenen

Systems gespeichert. Ein besonderes Augenmerk sollte auch auf die Mailkommunikation nach einem Sicherheitsvorfall gelegt werden. Vertrauliche Informationen sollten niemals ungesichert übertragen werden. Weiterhin sollte man immer daran denken, dass auch die Mailserver kompromittiert sein könnten oder der Angreifer den Netzverkehr belauschen könnte.

4.13 Anti-Forensik

Als Ermittler im Bereich der Computer-Forensik muss man sich auch bewusst sein, dass Tatverdächtige versuchen, ihre Spuren zu verschleiern oder die Datenanalyse zu behindern.

Sogenannte Anti-Forensik-Werkzeuge und -Technologien haben zum Ziel, die Datensicherstellung bzw. -analyse zu behindern oder gar unmöglich zu machen. Dies geschieht zum einen dadurch, dass für die Aufklärung relevante Informationen gelöscht bzw. verändert werden oder dass der Ermittler einfach nur abgelenkt oder aufgehalten werden soll. Da diese Anti-Forensik-Technologien auch mit einfachen Mitteln anwendbar sind bzw. entsprechende Werkzeuge frei verfügbar sind, sollte jeder Ermittlungsspezialist diese Technologien in den Grundzügen verstehen. Dies versetzt ihn in die Lage, auch wenn keine verwertbaren Spuren auf dem verdächtigen System mehr vorhanden sein sollten, wenigstens den Einsatz von Anti-Forensik-Tools nachzuweisen.

Anti-Detection vs. Anti-Forensik

Die Motivation zum Einsatz von Anti-Forensik-Werkzeugen oder -Methoden liegt hauptächlich darin, dem Administrator, dem originären Systemeigentümer oder den Ermittlern vorzugaukeln, dass nichts Verdächtiges stattgefunden hat. Computer-Forensik oder auch das Erkennen von Sicherheitsvorfällen basiert häufig auf Erkennung von Anomalien und Auffälligkeiten. Scheint das kompromittierte System normal, wird niemand Verdacht schöpfen und der Angriff bzw. das Delikt bleiben bei oberflächlicher Betrachtung unbemerkt. Bei genauerer Betrachtung kann zwischen Anti-Detection und Anti-Forensik unterschieden werden: Während bei der Anti-Detection Tat und Täter unerkannt bleiben sollen, möchte der Angreifer bei der Anti-Forensik die eigentliche Ermittlung behindern. Ein weiterer Grund für Anti-Forensik ist darin zu sehen, dass der Täter die Sammlung der relevanten Daten stören oder gar unterbinden möchte. Erreicht werden kann dieses Ziel auch, wenn der Ermittler aufgehalten und von wesentlichen Spuren abgelenkt wird. Dies ist besonders interessant, da gerade in großen, viel beschäftigen Ermittlungseinheiten nur ein gewisses Zeitkontingent für die Analyse zur Verfügung steht und der Angreifer den Ermittler eigentlich so lange aufhalten muss, wie die durchschnittliche, oft vom Management vorgegebene Analysephase, pro Fall dauert. Ist einem Täter bewusst, dass seine Taten auf Dauer nicht unentdeckt bleiben, oder will er sich auf eine mögliche Gerichtsverhandlung vorbereiten, kann es vorkommen, dass

er versucht, Nebelgranaten zu werfen, die als sehr offensichtliche Spuren in Erscheinung treten und die vom Ermittler, der froh ist, innerhalb seines eigenen Zeitfensters überhaupt etwas zu finden, zu leichtfertig aufgegriffen werden. Oft kann der Verdächtige im Nachhinein plausible Erklärungen für den Sachverhalt finden, deren Widerlegung durch den Ermittler weitere Analyseschritte bedürft hätte. Einem mit dem betroffenen Betriebssystem nicht vertrauten, unerfahrenen Ermittler kann es mitunter auch passieren, dass er die vielfältigen alternativen Möglichkeiten des Zustandekommens von digitalen Spuren nicht kennt und diese bei der Beweissicherstellung oder Analyse nicht bedenkt. Somit kann es einem erfahrenen kritischen Betrachter gelingen, Arbeitsweise und Integrität des unerfahrenen Ermittlers vor Gericht in Zweifel zu ziehen. Hat der Administrator die Tragweite des Sicherheitsvorfalls am Anfang unterschätzt, wurde wahrscheinlich eine lückenlose und manipulationssichere Sicherstellung der Beweisspuren ebenso versäumt wie die Erstellung einer forensischen Datenträgerkopie.

Angriff auf Werkzeuge

Gerade bei komplexen mehrstufigen Angriffen oder lange vorbereiteten Manipulationen von IT-Systemen möchte ein Angreifer im Vorfeld herausfinden, ob, wie und mit welchen Forensik-Werkzeugen die Ermittler arbeiten, natürlich ist es für ihn auch von Interesse, in welchen Netzbereichen sich die Ermittler befinden und wie die IPAdressen der Analysesysteme lauten.

Einige der verfügbaren kommerziellen, aber auch der freien Computer-Forensik-Werkzeuge, haben – vergleichbar mit anderen Softwareprodukten – Bugs und Sicherheitslücken. Hängt der Ermittler zu stark von diesen Werkzeugen ab oder hat er keine Zeit oder Möglichkeit, zusätzlich mit einem zweiten Werkzeug zu arbeiten, muss der Angreifer eigentlich nur diese Werkzeuge attackieren, um die gesamte Ermittlung zu torpedieren, den Ermittler zu frustrieren und den Zeitplan durcheinanderzubringen. Somit werden diese fehlerhaften Ermittlungstools dann zum eigentlichen Angriffsziel. Arbeiten die Ermittler nicht in geschützten Analyseumgebungen, kann ein Angriff möglicherweise großen Schaden anrichten, der bis zur Vernichtung bzw. Kompromittierung von Ermittlungsergebnissen führen kann. Abgesehen davon, dass der eigentliche Angriff unerkannt bleibt bzw. nicht aufgeklärt werden kann, könnte dies bei Bekanntwerden im Rahmen einer späteren juristischen Würdigung der Ermittlungsergebnisse zu einem erheblichen Vertrauensverlust führen. Der Angreifer möchte natürlich auch gern verschleiern, dass Anti-Forensik-Methoden zum Einsatz kommen, um dem Ermittler keinen Hinweis auf die auf der Angreiferseite vorhandenen Fähigkeiten zu geben. Vermutet der Ermittler leichtsinnigerweise ein Script Kiddy oder einen unerfahrenen Angreifer, würde er wahrscheinlich nur oberflächlich ermitteln.

Verschleierungsmethoden

Die einfachsten Anti-Forensik-Methoden (korrekterweise sind dies eher Anti-Detection-Methoden) bedürfen keines großen Tooleinsatzes und bestehen in der Regel darin, seine

Gebrauchsspuren regelmäßig zu löschen oder dafür zu sorgen, dass diese gar nicht erst entstehen.

Ein anderer Trend ist darin zu sehen, dass Anwender, die vielleicht im Verborgenen agieren wollen, vermehrt mit virtuellen Umgebungen arbeiten, um somit ihre Werkzeuge und Aktivitäten vor den Augen der IT-Administration zu verstecken. Für diese Zwecke kommen sowohl von USB-Sticks oder anderen externen Medien bootbare Betriebssysteme als auch externe Speicher im Internet zum Einsatz.

Datenträger-Löschsoftware

Eine andere Gruppe von Werkzeugen, die unter bestimmten Umständen auch im Bereich Anti-Detection angesiedelt werden kann, ist Datenträger-Löschsoftware. Diese Software dient ursprünglich dazu, Dateien und Verzeichnisse vollständig von einem Datenträger zu entfernen, sodass sie nur mit unverhältnismäßig hohem Aufwand wiederherstellbar wären. Aus Gründen des Informationsschutzes ist dies eine unbedingt zu empfehlende Sache. Geht es aber darum, herauszufinden, welche Daten von einem Verdächtigen von einer Festplatte gelöscht wurden, kann die Analyse extrem erschwert, in den meisten Fällen gänzlich unmöglich sein, wenn derartige Software zum Einsatz kam, da sie die auswertbaren Datenspuren zerstört. In diesen Fällen bleibt dem Ermittler nur übrig, zu beweisen, dass solche Datenträger-Löschsoftware zum Einsatz gekommen ist. Dann müssen sich Erkenntnisse über die mehr als ein Dutzend verfügbaren Löschsoftwareprodukte gewinnen lassen. Ein sicheres Indiz für die Verwendung von Löschtechniken ist natürlich der Nachweis des Vorhandenseins der Software selbst. Zum einen hinterlassen diese Werkzeuge ausgiebig Spuren während der Installation beispielsweise unter Windows – wie jede andere Windows-Software eben auch. Zum anderen erstellen einige Löschsoftwareprodukte Ereignisprotokolle, die manchmal selbst nach Deinstallation wiederherstellbar sind, da die Software zum sicheren Löschen ja dann nicht mehr vorhanden ist. Sind diese Hinweise auch nicht vorhanden, bleibt dem Ermittler nur übrig, die typischen Einsatzspuren der jeweiligen Löschsoftware zu finden. So arbeiten gerade im privaten Bereich häufig verwendete Löschsoftwareprodukte eben nicht mit zufälligen Löschpattern, sondern hinterlassen im freien Speicherbereich eindeutige Zeichenketten. Anhand dieser Zeichenketten, die für das Überschreiben der zu löschenden Informationen verwendet werden, lässt sich dann oft der Einsatz bestimmter Löschsoftwarevarianten bestimmen. Zu guter Letzt arbeitet die meiste Löschsoftware auch nicht so zuverlässig, dass sich nicht doch noch Gebrauchsspuren des Anwenders finden lassen, da gerade unter Windows an vielen Stellen Protokolle und Registry-Einträge erstellt werden. Hinzu kommt auch, dass viele Windows-Anwendungen Backup-Dateien oder Arbeitskopien in temporären Verzeichnissen anlegen, die von der Löschsoftware auch nicht immer vollständig erkannt und entfernt werden und dann mit Computer-Forensik-Werkzeugen wie z.B. File Carvern wiederhergestellt werden können.

Der Stecker sollte dann direkt am Gerät gezogen werden, damit eine eventuell übersehene USV nicht doch noch einen Shutdown initiiert.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Sonderzeichen