Forensik: Einbettung in präventive und reaktive Unternehmensprozesse

Nils Magnus

Best Practise Team Network Security and Incident Response
secunet Security Networks AG
Osterbekstr. 90b
D-22083 Hamburg
nils.magnus@secunet.com

Abstract: Die Computer Forensik kann dazu beitragen, dass Angriffe so analysiert werden können, um einerseits Systeme daraufhin besser abzusichern und andererseits den Verursacher aufzuspüren. Wesentliche Bedeutung hat dabei die organisatorische Vorbereitung der Untersuchung, um eine Vernichtung von wertvollen Hinweisen zu verhindern und Beweiskraft zu erhalten. Die praktische Ausführung besteht zum Großteil aus Arbeitsschritten, die einem erfahrenen Systemverwalter bekannt sind und die er einfach ausführen kann. Es gibt spezielle Werkzeuge für einzelne Aufgaben der Untersuchung. Der Beitrag gibt eine Übersicht der organisatorischen und technischen Maßnahmen und entwickelt mit einer Frageliste ein Vorgehensmodell für eine konkrete Analyse.

1 Einleitung und Motivation

Der Bereich der Computer Forensik ist interessanterweise ein Bereich, in dem in den letzten Jahren bemerkenswert wenig Fortschritt Einzug gehalten hat. Diese Spezialsparte rückte sich erstmals Ende der 80er Jahre des vergangenen Jahrhunderts in das Licht der Öffentlichkeit: Durch den Morris-Wurm [1] wurde erstmals die Belastbarkeit des damals noch jungen Internet auf die Probe gestellt und im Zuge des Datenverkaufes an den KGB [2] fand eine weitere, in Teilen tragische Geschichte weitläufige Beachtung. Beide Vorfälle sind gut dokumentiert [3], [4] machen aber auch das Dilemma deutlich, mit dem die Computer Forensik auch heute noch zu kämpfen hat: Technisch kann mit genügend Sachverstand vieles aufgedeckt werden; inwiefern dies vor Gerichten verwertbar ist, steht auf einem völlig anderen Blatt. In diesem Beitrag wollen wir aufzeigen, in welche Bereiche sich Computer Forensik heute aufteilt und was ein für die Sicherheit in einem Unternehmen, einer Behörde oder einer Organisation Verantwortlicher unternehmen sollte, wenn er in die Situation kommt, sich mit dem Thema beschäftigen zu müssen.

2 Computer Forensik

Beginnen wir mit dem Versuch einer Definition. Der Begriff „Forensik“ entstammt ursprünglich eher medizinischen bzw. kriminologischen Disziplinen. Im Wesentlichen geht es dabei um die Aufklärung von Vorgängen (häufig Verbrechen) anhand von Indizien, die am Zielobjekt des Vorganges (also üblicherweise des Opfers) noch vorgefun-

den werden. Diese Terminologie hat man dann später auch für Angriffe auf IT-Systeme und Netzwerke in Entsprechung angewandt. So definiert [5] *„Digitale Forensik ist die Aufbereitung von kriminellen Vorfällen im Zusammenhang mit Computern, zur Beweissicherung und zur Feststellung des Täters. Um Beweise zu sichern, werden z.B. Festplatten analysiert und Protokolle des Netzverkehrs gesichert."*

Die Begrifflichkeit ist dabei noch uneinheitlich, so finden sich die Begriffe „Digitale Forensik", „Electronic Forensics" oder „Computer Forensik". Wir werden im Weiteren den letzten Begriff verwenden und dabei manchmal nur von „Forensik" sprechen, wenn der Kontext eindeutig ist.

Die Computer Forensik ist mit einer Reihe von weiteren Spezialdisziplinen verwandt oder eng verknüpft: Die technischen Methoden des *Penetration Testing* sind oft denen der Computer Forensik sehr ähnlich, wenn auch jeweils ein anderer Anwendungsfall vorliegt: Wird beim Penetration Testing präventiv ein Angriff simuliert, so muss in der Computer Forensik ein geschehener Angriff nachvollzogen werden. Das jeweilige technische Wissen ist dabei oft sehr hilfreich. Ebenfalls auf technischer Ebene ist die *Intrusion Detection* sehr eng mit der Computer Forensik verknüpft, da einerseits ID-Systeme wertvolle Daten liefern können, die eine forensische Auswertung erst möglich machen oder essentiell ergänzen, aber auch, weil in beiden Fällen zumindest teilweise mit a priori unbekannten Umständen und Methoden umgegangen werden muss.

Eine weitere Nische innerhalb der Computer Forensik ist die *Data Recovery*, in der versucht wird, von unterschiedlichen Medien beweisrelevante Daten zu extrahieren. Diese in Teilen schon in die Feinmechanik und andere Ingenieursdisziplinen hineinspielende Tätigkeiten bieten mittlerweile dutzende von Unternehmen als Spezialdienstleistung an. Dabei können Daten sowohl von Festplatten diversen Wechselträgern wie CDROM, DVD oder anderen Disks oder von magnetischen Datenträgern wie Disketten oder Datensicherungsbändern restauriert werden.

Auf organisatorischer Seite ist die Computer Forensik oft zunächst in die Prozesse des *Incident Response* eingebettet: Wird ein Angriff auf IT-Systeme erkannt, gilt es oft in erster Linie, den entstandenen Schaden zu begrenzen und die Ursache des Angriffes zu unterbinden. An dieser Stelle sollte im Sinne einer nachhaltigen Strategie jedoch nicht innegehalten werden, sondern versucht werden, ebenfalls den Verursacher ausfindig zu machen, um potentielle *Regressansprüche* durchzusetzen, eine *Strafanzeige* einzuleiten oder zukünftig ähnlich gelagerte Angriffe besser zu unterbinden. Diese Vorgehensweise hat sich jedoch noch nicht in weitem Maße durchgesetzt, gerade das verantwortliche Management scheut hier häufig den denkbaren Imageverlust. Dabei hat sich gezeigt, dass bei fundiertem und kompetentem Vorgehen gegen Angreifer dessen Aktivitäten im Rahmen des bereits entstandenen Schadens durchaus ins Positive umgemünzt werden können, da so unmissverständlich demonstriert werden kann, dass IT-Sicherheit wirklich ernst genommen und konsequent betrieben wird.

Solche ein Vorgehen ist jedoch nur dann möglich, wenn sowohl Incident Response als auch die Computer Forensik klar in die Unternehmensprozesse, insbesondere das *Sicherheitsmanagement* eingebettet ist und dafür die notwendigen Ressourcen bereitgestellt werden.

Wenn Computer Forensik in einem normalen Unternehmenskontext eingesetzt werden soll, sind zumeist einige Abgrenzungen notwendig, da bestimmte Verfahren ein unverhältnismäßig hohes Maß an Spezialwissen, -werkzeugen oder Systemleistung erfordern, das nur in Sonderfällen vorgehalten werden kann. Solche Aufgaben bleiben aus wirtschaftlicher Betrachtung heraus besser Spezialisten überlassen. So können gelöschte Daten, selbst dann von Festplatten restauriert werden, wenn sie mehrfach und mit zufälligen neuen Inhalten überschrieben wurden: Wenn man unter einem Rasterstrahlmikroskop die Magnetspuren sichtbar macht, lassen sich durch differierende Spurlagen im Mikrometerbereich oder darunter noch Daten restaurieren. Verschlüsselte Datenbereiche, die ein Angreifer hinterlassen hat, können je nach eingesetztem Verfahren mitunter durch den Einsatz von Numbercrunchern im Brute-Force-Verfahren dechiffriert werden. Solche Verfahren sind möglich, sollen hier jedoch als High-End-Forensik nicht eingehender betrachtet werden.

Der verbleibende Anteil, der sicherlich den die ganz wesentliche Mehrheit aller Vorfälle abdeckt, lässt sich dabei in drei Bereiche aufteilen. Für die praktische Durchführung sind Kenntnisse allen drei Bereichen notwendig:

- Allgemeine gute Kenntnisse von Anwendungen, Systemen und Netzwerken,
- Methodische Kenntnisse, d.h. Methoden und Werkzeuge, die spezifisch für die Computer Forensik sind, sowie
- die Betrachtung von organisatorischen Fragen zur Vorbereitung und Durchführung von forensischen Untersuchungen.

Alle drei Bereiche sollen in den folgenden Abschnitten näher betrachtet werden.

3 Allgemeine Kenntnisse

Die Computer Forensik setzt eine Menge „Spürsinn“ voraus. Daher mag ein Vergleich mit Detektiven erlaubt sein: Dessen Hilfsmittel sind zwar notwendig, aber ein Großteil der Arbeit macht „logisches Schlussfolgern“ aus.

Daher sind sehr solide Fachkenntnisse der am „Tatort“ eingesetzten Technologie unverzichtbar. Eine weitere wichtige Eigenschaft ist eine gewisse Kreativität, um neue Wege einzuschlagen, da für die anstehende Aufgabe ja explizit kein Handbuch oder Pflichtenheft zur Verfügung steht. Schließlich müssen während einer Untersuchung optimalerweise sowohl die Motivation als auch die Vorgehensweise des Angreifers nachvollzogen werden.

Am einfachsten sind noch die Fachkenntnisse zu trainieren, die anderen beiden Eigenschaften zu erwerben, wenn man sie nicht hat, kann sich als schwierig erweisen. Hinsichtlich der Fachkenntnisse sollte man in der Lage sein, die wichtigsten zustandsgebenden Komponenten eines Systems einzuschätzen und zu bewerten. Dazu gehören hauptsächlich die im Folgenden beschriebenen Komponenten.

3.1 Betriebssystem

Der Aufbau des Betriebssystems muss gut bekannt sein, um Änderungen schnell und sicher zu erkennen. Eine Absicherung durch *Integritätstester* wie **tripwire**, welches mit MD5-Hashwerten mögliche Modifikationen aufzeigt, kann hier nützlich sein. Solch ein Verfahren ist allerdings nur dann verlässlich, wenn die Prüfsummen auf einem gesonderten, nicht mit dem System verbundenen Datenträger gesichert wurden.

Weiterhin kann so gewissenhaft eingeschätzt werden, ob alle vorgefundenen Dateien wirklich ihren scheinbaren Zweck erfüllen. Dies gilt insbesondere für Treiber, nachladbare Betriebssystemmodule, aber durchaus auch für Konfigurationsdateien und auch ausführbare Programme. Gerade für Letztere kann das Tool **strings** wertvolle erste Anhaltspunkte in binären Dateien liefern, da es häufig feste Textbausteine, die der Angreifer hinterlassen hat, extrahieren kann. Auf diese Weise kann gelegentlich eine E-Mail- oder Web-Adresse ausfindig gemacht werden, an die ein Trojaner seine Daten zu senden versucht.

Eigene (Grundlagen-) Kenntnisse der Programmierung sind insofern nützlich, um Probleme und Vorgehensweisen z. B. mit Prozessrechten und User-IDs besser einschätzen zu können. Das komplexe Thema der SUID- und GUID-Flags ist ein Beispiel dafür.

3.2 Prozesse und Hauptspeicher

Neben den dauerhaft gespeicherten Resten eines Angriffs darf man die aktuell im Hauptspeicher befindlichen Prozesse nicht vergessen. Hier gibt es teilweise aufwändige Tarntechniken, die genau diese Dinge verschleiern sollen. Ein noch laufendes Programm kann auf der Festplatte längst gelöscht sein. Wie [6] zeigt, kann sich gerade in Server-Systemen ein Stück Code über viele Tage im Seitenspeichercache halten; wenn es noch aktuell läuft, zwangsläufig noch darüber hinaus. Hier kann **lsof** gute Dienste leisten. Umfassende Übersichten zu laufenden Prozessen liefert **ps** (es ist wichtig, die Authentizität des Programms zu gewährleisten!). Wo möglich, sollte man die Anfertigung eines kompletten Speicherabbildes in Betracht ziehen (z. B. mittels **dd if=/proc/kcore** unter Linux). Solange jedoch das vom Vorfall betroffene Betriebssystem selbst zur Durchführung irgendwelcher Sicherungsmaßnahmen benutzt wird, muss davon ausgegangen werden, dass der Zustand des Systems verändert wird. Hier kann es in dem Falle nur noch darum gehen, diese Modifikationen nachvollziehbar und so gering wie möglich zu halten.

3.3 Dateisystem

Das Dateisystem, das zumeist auf Massenspeichern wie Festplatten zu finden ist, enthält oft die wichtigsten Anhaltspunkte für das Vorgehen des Angreifers. Es sollte daher nach unterschiedlichen gesichtspunkten untersucht werden: Methoden zum Auffinden von unerwünschten Programmen oder Dateien sind wichtig, um die spätere Rückkehr des Angreifers in das System zu verhindern. Die Analyse von Zeitstempeln erlaubt es mitunter, die zeitliche Abfolge des Angriffes zu rekonstruieren und daraus Schlüsse für ein weiteres Vorgehen zu ziehen. Ebenfalls durch die Zeitstempel kann abgeschätzt werden,

welche Dateien und damit welche Daten und Dokumente überhaupt einer Manipulation unterworfen wurden. Vorsicht ist hier nur insofern angebracht, als dass sich diese Zeitstempel vergleichsweise einfach fälschen lassen. Mindestens eine Plausibilitätskontrolle und eine Korrelation mit anderen Daten sind notwendig, um dieses Argument nicht sofort zu entkräften. Wichtige Programme sind in diesem Zusammenhang **find** *(*insbesondere mit den diversen Suchprädikaten für Änderungs- und Zugriffszeiten), **chmod** und **chown, ls** und **touch**.

3.4 Logfiles

Bei den meisten Angriffen nutzt der Angreifer keinen direkten Zugriff auf das physikalische System (in dem Fall ist eine forensische Analyse ohnehin wesentlich schwieriger, da noch physikalische Manipulationen betrachtet werden müssen), sondern verschafft sich Zugang über ein Netzwerk. Solche Aktivitäten werden in diversen Logdateien protokolliert. Sofern diese plausibel und authentisch sind, können sie ebenfalls einen gewissen Aufschluss über das mögliche Vorgehen bieten. Ob sich eine verfahrenstechnische Argumentation erfolgreich alleine auf Logfiles ohne besondere Signierung stützen kann, ist jedoch sehr unwahrscheinlich. Insofern muss auch hier die Manipulation an Logfiles für aussagekräftige Ergebnisse möglichst ausgeschlossen werden.

Können hier jedoch Logfiles von mehreren Systemen kombiniert werden, die auch hinsichtlich ihrer Vertrauensstellung untereinander unabhängig sind, so kann die Beweiskraft gestärkt werden. Hier sind z. B. auch Router-Flow-Dumps [7] oder SNMP-Trap-Logs mitunter hilfreich.

3.5 Netzwerkzugriffe

Weit häufiger also erfolgt der Zugriff über Netzwerke. Daher ist es notwendig, schnell und sicher den Ausgangspunkt des Angreifers ausfindig zu machen, da häufig nur so seine tatsächliche Identität aufgedeckt werden kann. Doch gerade diese Untersuchungen erweisen sich häufig als schwierig. Zeigt **netstat** noch die aktuellen und zuletzt genutzten Verbindungen zum untersuchten System an, so sind dies doch zunächst nur IP-Adressen, die ohnehin mit einem gewissen Aufwand gefälscht sein können. Dabei sind netzwerktopologisch „nahe“ Adressen oft einfacher z. B. durch ARP-Spoofing [8] zu fälschen als weiter entfernte, obwohl auch dies nicht unmöglich ist [9]. Gerade bei andauernden Untersuchungen, bei denen der Angreifer live beobachtet werden kann, ist ein Mitschnitt des verursachten Netzwerkverkehres oft sehr aussagekräftig. Dazu gut geeignet ist das Programm **tcpdump**. Wenn solche Daten ausgewertet werden, ist unbedingt darauf zu achten, dass nicht nur der eingehende, sondern auch der ausgehende Netzverkehr beobachtet wird. Einige Angreifer installieren zeitgesteuerte Komponenten, die regelmäßig oder zu bestimmten festgelegten Zeitpunkten von sich aus die Verbindung mit einem System oder Netzwerk des Angreifers suchen. So verbinden sich viele durch Windows-Viren verbreitete Programme zu anonymen Chat-Foren und nehmen dort vom ursprünglichen Angreifer nach dessen Authentisierung mit einem Passwort Kommandos entgegen (sog. *Bot-Nets*).

4 Werkzeuge und Methoden

Vielleicht zunächst überraschend, stellt man schnell fest, dass es nur wenige spezifische Werkzeuge zum Einsatz in der Computer Forensik gibt. Betrachtet man jedoch im Vergleich die Hilfsmittel eines kriminologischen Forensikers, so stellt man fest, dass auch er hauptsächlich die Werkzeuge und Methoden der Medizin und einiger anderer Disziplinen in geeigneter Weise einsetzt. Auch in der Computer Forensik ist dies nicht viel anders. Dennoch existiert eine Reihe von Programmen, die speziell zur Analyse von Angriffsüberresten entwickelt wurden. Hier soll eine Auswahl dieser Werkzeuge vorgestellt werden, die zum Großteil als Open Source verfügbar sind. Eine detailliertere Liste einzusetzender Tools wird sich aus jedem konkreten Vorfall ergeben müssen.

4.1 Werkzeuge

Das erste Programmpaket, das sich explizit der Thematik der Forensik angenommen hat ist TCT, „the Coroner's Toolkit“ [10]. TCT ist kein einzelnes Programm, sondern eine Sammlung von Einzelwerkzeugen in einer Umgebung, die besonders auf die Anforderungen der Forensischen Analyse abgestimmt ist. So werden von allen Kommandos die jeweilige Start- und Endzeit automatisch mitprotokolliert. Kernpunkt der Toolsammlung ist die Analyse von Dateisysteminformationen, obwohl auch viele andere Einzelangaben erhoben und zur späteren Untersuchung gesichert werden. Dazu legt im praktischen Einsatz das Programm **grave-robber** einen so genannten *Body* an, eine Art Datenbank, in der Angaben über Dateien, Änderungen und Löschungen abgelegt werden. Weiterhin wird eine große Anzahl von weiteren Angaben, die in den vorangegangenen Abschnitten schon angesprochen wurden in Dateien durch die zugehörigen Unix-Kommandos gesichert. Dabei ist es erklärtes Ziel, die forensischen Daten von einem System erst einmal in definierter Weise zu erheben; die konkrete Auswertung muss im Nachgange von Hand auf Grundlage der gesammelten Informationen geschehen.

Eine Weiterentwicklung insbesondere der Dateisystemkomponente von TCT ist TASK, welches seit einiger Zeit gemeinsam mit der grafischen und browsergeführten Oberfläche **autopsy** unter dem Namen *Sleuthkit* [11] firmiert. Mittels **autopsy** können so Untersuchungen neu angelegt und verwaltet werden. Hier werden mittlerweile eine ganze Reihe von spezifischen Dateisystemen unterstützt, darunter die wichtigsten im Linux- und Unix-Umfeld aber auch beispielsweise NTFS. Dazu können dann Detailinformationen zu einzelnen Objekten, Zugriffs- und Änderungsdaten abgerufen, Inhalte betrachtet und sogar automatisiert Änderungshistorien angelegt werden. Hilfreich ist, dass die Untersuchungen auch auf mittels **dd** erzeugten Abzügen von Festplatten operieren können.

Bei unbekannten vorgefundenen Dateien können die diversen *Signaturdatenbanken*, z.B. Known Goods[12] oder die NIST National Software Reference Library (NSRL) [13] eine erste Hilfe sein. Hier werden Signaturen sowohl bekannter gut- wie bösartiger Software vorgehalten, um auf diese Weise schnell vorklassifizieren zu können, was für Dateien sich auf dem untersuchten Datenträger finden. Wenn jedoch keine bekannten Signaturen gefunden werden, ist es nötig, Reverse-Engineering zu betreiben, wenn die Funktionalität des Programms herausgefunden werden soll. Die Werkzeuge **strings** oder

od können dazu schon erste Erkenntnisse liefern; weiterführende Maßnahmen sprengen allerdings den Rahmen dieses Beitrages.

Somit liegt eine Reihe von spezifischen forensischen Werkzeugen vor; es bleibt jedoch zu betonen, dass alle diese Werkzeuge nur dann sinnvoll einzusetzen sind, wenn sich der mit der Untersuchung Betraute bereits vor einem Vorfall mit den Systemen beschäftigt hat. Die Installation und Bedienung der Werkzeuge ist keineswegs trivial und ein unglücklicher Testlauf an einem „heißen System" würde potentiell viel zu viele Spuren vernichten.

So bietet sich also an, den Fall der Fälle vorher einmal zu proben. Insbesondere das Aufspielen der Software kann sich komplex gestalten, denn es kann ja nicht a priori von der Integrität gegebenenfalls vorinstallierter Software ausgegangen werden. Hier kann Knoppix, ein von CDROM oder DVD startendes Linux-System gute Dienste leisten. Eine Übersicht weiterer Forensik-Werkzeuge in einem für den mit der Durchführung in praktischer Weise umgebenden Verpackung ist Knoppix-STD, eine angepasste Version der bootfähigen Linux-Distribution. Wenn ein System bereits heruntergefahren wurde oder als Image vorliegt, können auf diese Weise auch andere Betriebssysteme als Linux untersucht werden.

4.2 Rückverfolgung

Bei der *Rückverfolgung* des Angreifers sind viele hohe Hürden zu überwinden: Zunächst ist die Ermittlung der IP-Adresse, von der aus ein Angreifer eine Verbindung zum untersuchten Objekt hergestellt hat mittels den eben erwähnten Tools schnell ausfindig gemacht. Durch eine geeignete Kombination aus **traceroute** und eine Abfrage der **whois**-Datenbank mit dem gleichnamigen Werkzeug kann auch eine grobe Abschätzung der räumlichen Lokalisierung des Angreifers geschehen. Doch hierbei ist große Vorsicht vor vorschnellen Schlüssen geboten, denn diese Datenbanken geben mitunter auch veraltete Auskünfte oder aber der Angreifer hat sich von einem völlig anderen Teil der Welt dort eingewählt.

Möchte man also den wirklichen Ursprung des Angreifers herausfinden, so müssen die Analysen auf dieses und in transitiver Weise auf alle davorliegenden Systeme ausgeweitet werden. Dies wird zumeist nur dann möglich sein, wenn bereits Kontakte zu den Systemverantwortlichen dieser Knoten besteht oder schnell hergestellt werden können. Dieser Problematik nimmt sich u. a. seit einigen Jahren das Forum of Incident Response Teams (FIRST) [14], eine Art weltweiter Dachverband von CERTs (Computer Emergency Response Teams) an, so dass eine Mitgliedschaft oder ein guter Kontakt zu dieser Vereinigung sich ebenso nützlich erweisen kann, wie Kontakte zu lokalen, nationalen und internationalen Ermittlungsbehörden.

4.3 Gerichtsverwertbarkeit

Gegenwärtig besteht eine sehr unklare Situation darüber, was als geeignetes Regelwerk für gerichtsverwertbare Beweise oder Indizien gelten kann und was nicht vor Gericht akzeptiert wird [15]. Es sollte jedem in forensische Analysen Beteiligtem klar sein, dass

es mitunter große Diskrepanzen zwischen technischer Sicht und der Auffassung eines Kriminalbeamten oder eines Gerichts geben kann. Als Grundsatz gilt jedoch, dass alle Untersuchungen so weit wie nur irgend möglich von allen Beteiligten nachvollzogen werden müssen. Daher sind besondere Anstrengungen in das Protokollieren und Dokumentieren aller Untersuchen zu stecken.

Am sichersten geht man dabei, wenn alle Untersuchungen wiederholbar und nur auf Kopien der tatsächlich vorgefundenen Daten durchgeführt werden. Die Orginalkopien sollten so früh als nur möglich in unabhängige Hände gegeben werden, um sich so vor einem Manipulationsvorwurf schützen zu können.

Regelwerke zum praktischen Vorgehen werden von verschiedener Stelle gegenwärtig erarbeitet [16], [17], aber noch hat sich kein solches Verfahren auch einem wirklichen Praxistest stellen können. Dennoch bleibt zu hoffen, dass auf diesem Gebiet die Strafverfolgung und die technisch verantwortlichen Experten hier in nächster Zeit verwertbare Ergebnisse generieren.

Zuletzt bleibt bei der Durchführung von Forensischen Analysen noch der Hinweis, dass auch andere Rechtsbereiche in erheblicher Weise berührt werden können, so insbesondere der Datenschutz oder innerbetriebliche Regelungen. Es ist bei einer Untersuchung darauf zu achten, ob Persönlichkeitsrechte sowohl des Angreifers als auch unbeteiligter Dritter verletzt werden würden oder wie mit kollateral zur Kenntnis gelangten personenbezogenen Informationen umzugehen ist.

5 Organisatorisches

Der organisatorischen Planung einer forensischen Analyse kommt oft eine viel größere Bedeutung zu, als dies zunächst erscheint. Denn in einer Vielzahl von Fällen werden aus Unachtsamkeit oder aus scheinbaren operativen Notwendigkeiten heraus wichtige Beweise vernichtet, die später zum Regress gegen den Verursacher genutzt werden könnten.

Eine gute Vorbereitung, die durch gelebte Policies unterstützt wird, ist deshalb so wichtig, da in den meisten Fällen die „Entdecker“ eines Angriffs nicht identisch mit dem Personenkreis sind, der die forensischen Untersuchungen vornimmt. In einer Policy sollten also einerseits allgemein verständliche Anweisungen stehen, was bei Entdecken eines Angriffes zu tun und zu unterlassen ist, und andererseits, wer in welcher Form zu benachrichtigen ist. An dieser Stelle ist zu bedenken, dass der Angreifer ggf. die Kommunikationsmittel wie z. B. E-Mail bereits mithört und monitort.

Jedoch ist gerade in der frühen Phase der Entdeckung die Gefahr am größten, dass wichtige Hinweise vernichtet werden. Ein oft als Allheilmittel angesehener Reboot des Systems kann aufschlussreiche Prozesse beenden, Logfiles oder temporäre Dateien löschen. Eine gute Faustregel ist, nach dem Entdecken des Angriffes die Verbindung zum Netz umgehend durch das Ziehen der Netzwerkkabel zu unterbrechen, ansonsten aber das System unverändert zu lassen. Es sollten weder Login- noch Logoutversuche unternommen werden, keine Konfiguration geändert und keine Untersuchung gestartet

werden, bis das Forensik-Team benachrichtigt wurde und seine Arbeit aufgenommen hat.

Als erstes muss entschieden werden, ob der Angriff abgebrochen werden soll. Wenn die Notwendigkeit hoch ist, den Angreifer nachweislich zu überführen, kann es hilfreich sein, dessen weitere Schritte zu beobachten, um so dessen Identität und Beweggründe in beweisbarer Form aufzuzeichnen.

In allen Fällen sollte so früh wie möglich ein unveränderliches Abbild der Ausgangssituation aufgezeichnet werden. Optimalerweise wird dieses Abbild im Beisein eines Notars aufgezeichnet oder später einem solchen übergeben, der es verwahrt. Dabei ist darauf zu achten, dass so wenig Information wie möglich durch den Akt des Kopierens verloren gehen. Ein einfaches Kopieren von einer Festplatte auf eine neue ändert potenziell das Zugriffsdatum aller Dateien. Am günstigsten ist es, die Rohinformation der kompletten Partitionen und ihre Geometriedaten zu sichern (z. B. mit dem Werkzeug **dd**). Auf gleiche Weise kann man mit dem Hauptspeicher vorgehen, wenn das Betriebssystem eine geeignete Schnittstelle bietet. So könnte man mit **dd if=/proc/kcore** auf einem Linux-System einen Dump des virtuellen Hauptspeichers machen.

Die oberste Maxime sollte daher sein, Analysen nur auf Kopien durchführen. Um diese anzulegen bietet sich eine Netzverbindung an, um die Rohdaten auf ein Sicherungssystem zu überspielen. Hier kann das zum Netcat-Paket gehörende **nc** wertvolle Hilfe leisten.

Um den Ablauf einer forensischen Analyse, die häufig ungeplant und unter Zeitdruck durchgeführt werden muss, besser zu strukturieren, wurde eine Liste von Kontrollfragen entwickelt, die gemeinsam vom Entdecker und dem Forensik-Team beantwortet werden sollten:

- Wie wurde der Angriff bemerkt? Welche Gegenmaßnahmen sind bereits und von wem durchgeführt worden?
- Welche Daten wurden vom Angreifer verändert? Hat er zusätzliche Software installiert oder Konfigurationen geändert (Backdoors)?
- Wie kann diese Veränderung bewiesen werden? Liegen Sicherungskopien vor dem ersten Angriff vor?
- Wann war der erste Zeitpunkt des Angriffes, der nachgewiesen werden kann? Sind die Daten vor dem Datum definitiv unkompromittiert?
- Wie war der zeitliche Ablauf des Angriffes? Lassen sich Aussagen über Abstände der Angriffe oder Tageszeiten machen?
- Lässt sich aus diesen Angaben ein Motiv des Angreifers ablesen? Sollten betriebswirtschaftliche Daten abgerufen oder verändert werden oder war der Angreifer eher von technischem „Spieltrieb“ motiviert?
- Bestehen Vertrauensbeziehungen vom untersuchten System aus zu anderen lokalen Systemen, die damit ebenfalls kompromittiert sein könnten?

- Kann der ursprüngliche Ausgangspunkt (sowohl auf Netzwerk-Ebene als auch geografisch) ermittelt werden? Wer sind die jeweiligen Ansprechpartner (Systembetreiber und Ermittlungsbehörden) am Ausgangspunkt?

- Welche Stellen wurden bereits informiert, welche müssen noch informiert werden? Dazu können IT-Verantwortliche, Systemverwalter, IT-Sicherheitsbeauftragte, Datenschutzbeauftragte, Incident-Response-Teams oder Polizei/Staatsanwaltschaft gehören.

6 Fazit

Mit der richtigen Vorbereitung sowohl auf organisatorischer wie technischer Ebene lässt sich ein Angriff auf Computersysteme aufklären und oft auch der Verursacher ermitteln, wenn alle Informationen genutzt werden. Es gibt erste Ansätze, um die Anforderungen von Ermittlungsbehörden an gerichtsverwertbare Beweise zu definieren, aber hier fehlen noch verbindliche Vorgaben und mehr praktische Erfahrungen in der Rechtssprechung.

7 Literaturverzeichnis

[1] Eugene Spafford: The Internet Worm Program: an Analysis (Purdue CS Technical Report TR-CSD-823)

[2] Clifford Stoll: The Cuckoos's Egg. Doubleday, New York, NY, 1989.

[3] Freke Over et. al.: Dokumentation über Karl Koch, Berlin 1989, als Digitale Kopie unter http://www.schaechl.de/kk/

[4] William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin: Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition 2003, Addison Wesley.

[5] Inside Security IT Consulting GmbH: Definition Digitale Forensik, 2003, http://www.inside-security.de/digitale_forensik.html

[6] Wietse Venema: Memory Forensics, FIRST Technical Colloquium, Uppsala, 2003

[7] Rob Thomas: Tracking Spoofed IP Addresses, http://www.cymru.com/Documents/tracking-spoofed.html

[8] Alberto Ornaghi, Marco Valleri: Ettercap, http://ettercap.sourceforge.net/

[9] Matthew Tanase: IP-Spoofing, An Introduction; Security Focus, 2003, http://www.securityfocus.com/infocus/1674

[10] Wietse Venema, Dan Farmer: The Coroner's Toolkit, http://www.porcupine.org/forensics/tct.html

[11] Brian Carrier: The Sleuth Kit Informer, Issue #1, 2003, http://www.sleuthkit.org/

[12] Known Goods Database, http://www.knowngoods.org/

[13] National Institute of Standards and Technology: National Software Reference Library (NSRL), http://www.nsrl.nist.gov/

[14] Forum of Incident Response and Security Teams (FIRST), http://www.first.org/

[15] Helmut Rüßmann: Moderne Elektroniktechnologie und Informationsbeschaffung im Zivilprozeß; Veröffentlichungen der Wissenschaftlichen Vereinigung für Internationales Verfahrensrecht, Band 8, 1997, S. 137 bis 205

[16] Cyber Tools On-Line Search for Evidence, EU funded project, http://www.ctose.org/

[17] D. Brezinski, T. Killalea: Guidelines for Evidence Collection and Archiving; RFC 3227, February 2002

8 Über den Autor

Nils Magnus studierte Informatik und Physik an der Universität Kaiserslautern, wo er als Diplom-Informatiker in der Arbeitsgruppe für Wissenbasierte Systeme graduierte. 1995 begründete er mit anderen den LinuxTag, die heute führende Konferenz und Messe um das Thema Linux und freie Software und ist heute ihr Program Chair.

Nach Tätigkeiten als freiberuflicher Entwickler und Software-Architekt sowie als Dozent für Networked Computing und System Management arbeitet er seit 1999 als Senior-Berater für Informationssicherheit bei der secunet Security Networks AG in Hamburg. Dort entwickelt er für Kunden Incident Response Lösungen und organisiert, plant und führt Projekte im Bereich der Schwachstellenanalyse durch.

In seiner Freizeit reist er gerne in verlassene Wüsten und große Städte, versucht sich sowohl an Italienischer Sprache wie Küche und schätzt den intellektuellen Kitzel durchdachter Musik.