Einleitung

»Ich brauche Informationen, Watson!«

Sicherheit in der Informationstechnik stellt ein wachsendes Problem dar. Hiermit ist natürlich nicht die Sicherheit an sich gemeint, sondern die Gefährdung der Sicherheit, die sich aus Unwissenheit, Fahrlässigkeit oder Vorsatz ergibt. Fast jede Organisation ist durch den massiven Einsatz von Informationstechnologie auch von ihr abhängig. So enthalten Computersysteme heute immer mehr und besser verdichtete Daten, die für den reibungslosen Ablauf von Geschäfts- und Arbeitsprozessen notwendig sind. Diese Abhängigkeit von der Informationstechnologie macht die betroffenen Einrichtungen zu einem idealen Ziel für Angreifer und Störenfriede.

Firewalls und Intrusion-Detection-Systeme

Die Sicherheitsverantwortlichen haben die Entscheidungsträger in den Unternehmen mittlerweile davon überzeugt, dass bei bestimmten Netzschnittstellen Firewall-Systeme halbwegs sichere Kommunikationsszenarien ermöglichen. Nachdem dieser Lösungsansatz gerade bei immer komplexeren Anwendungsstrukturen nicht immer konsequent umsetzbar erschien, wurden in einem weiteren Schritt häufig Intrusion-Detection-Systeme (IDS) installiert; sie sollen jene Angriffe erkennen, die mit Firewalls nicht zu verhindern sind. Es geht heute also nicht mehr nur darum, das Auftreten eines Sicherheitsproblems zu verhindern.

Es geht vielmehr darum, auch dann noch eingreifen zu können, wenn die ersten Schutzmechanismen von einem Angreifer überwunden wurden: Ein gerade ablaufender oder bereits eingetretener Sicherheitsvorfall muss zuverlässig erkannt werden, seine Auswirkungen sind wirksam einzudämmen, und es sollten dabei genügend Informationen gesammelt werden, um später eine sinnvolle Täterermittlung zu ermöglichen.

Forensische Untersuchungen

Zumeist sind also kombinierte Gegenmaßnahmen nötig, um auf Sicherheitsvorfälle zu reagieren. Dazu gehören auch die sogenannten

forensischen[1] Untersuchungen. Sie finden in der Regel dann statt, wenn es ernst zu nehmende Hinweise auf erfolgte oder gerade ablaufende Angriffe bzw. andere strafbare Handlungen auf die eigene Systemlandschaft gibt.

Der Begriff Computer-Forensik oder auch Digitale Forensik hat sich in den letzten Jahren für den Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität durchgesetzt. In Anlehnung an die allgemeine Erklärung des lateinischen Worts Forensik ist die Computer-Forensik ein Teilgebiet, das sich mit dem Nachweis und der Aufklärung von strafbaren Handlungen z.B. durch Analyse von digitalen Spuren beschäftigt.

Wer sollte dieses Buch lesen?

Fast jede Organisation wurde bereits mit der Frage eines erfolgreichen Systemeinbruchs konfrontiert, und auch Privatpersonen, die ihren PC mit dem Internet verbinden, können Opfer eines Angriffs werden. Die wenigsten sind aber darauf vorbereitet. Will man Sicherheitsprobleme vermeiden oder ermitteln, ob noch andere Systeme der eigenen Umgebung Opfer eines Angriffs geworden sind, ist es sinnvoll, forensische Untersuchungen durchzuführen. Hierbei geht es u.a. darum herauszufinden, ob ein Angreifer wirklich erfolgreich war, welchen Weg er genommen hat und welche Systemlücken zu diesem Einbruch geführt haben könnten. Das Internet und aktuelle IT-Publikationen sind voll von Tipps und Tricks zum Absichern von Systemen und Kommunikationswegen, viele Dinge werden von den Administratoren umgesetzt, dennoch kommt es zu Einbrüchen.

Administratoren

Dieses Buch soll auch dem technisch versierten Administrator einen ersten Überblick geben, welche Maßnahmen sinnvoll sind und welche Werkzeuge und Methoden ihm zur Verfügung stehen. Die meisten technischen Zusammenhänge sind diesem Personenkreis aus der täglichen Arbeit bereits geläufig. In der Praxis ist aber häufig zu beobachten, dass bei der konkreten Behandlung von Sicherheitsvorfällen trotzdem oftmals Unwissenheit vorherrscht und Fehler gemacht werden. Dieser Lesergruppe werden Grundlagen und Hintergründe bei der Erkennung und Analyse von Systemeinbrüchen vermittelt. Außerdem erfahren Sie Wissenswertes über die Zusammenarbeit mit Ermittlungsbehörden.

Sicherheits- und IT-Verantwortliche

Leser, die über keinen intensiven technischen Hintergrund verfügen, aber für die Erstellung von Handlungsanweisungen und Richtli-

1. forensisch [lat.]: gerichtlich oder auch kriminaltechnisch; z.B. auch forensische Medizin, forensische Psychologie

nien verantwortlich sind, können hier weitere Erkenntnisse über die Möglichkeiten der Computer-Forensik und Incident Response[2] sammeln. Diese Erkenntnisse können die Basis für eigene Konzepte bei der Behandlung von Sicherheitsvorfällen bilden. Weiterhin erfährt dieser Leserkreis, welche Fähigkeiten (»Skill-Profile«) und organisatorischen Rahmenbedingungen für eigene Ermittlungsteams notwendig sind.

Strafverfolger und Ermittler

Lesen sollten dieses Buch auch Ermittler aus dem Strafverfolgungsumfeld, die die Werkzeuge und Methoden für die Erfassung und Auswertung von Beweisspuren besser verstehen und bewerten möchten. Der Blick für die technischen Möglichkeiten bei der Ermittlung hilft, die eingesetzten Verfahren bzw. gefundenen Beweisspuren sowie deren Grenzen besser einzuschätzen. Die Kenntnis, wie die Spuren gefunden werden und was sie eigentlich aussagen, kann für die spätere Bewertung durchaus hilfreich sein.

Alle o.g. Lesergruppen erhalten einen Überblick über die Methoden zur Erkennung von und der Spurensuche nach Systemeinbrüchen. Die IT-Spezialisten werden sicherlich mehr interessante und neue Erkenntnisse aus dem Bereich des richtigen Umgangs mit Beweismitteln und den Entscheidungen zur weiteren juristischen Verfolgung gewinnen können. Strafverfolger werden den hier gelieferten Überblick über die technischen Möglichkeiten der Beweisgewinnung zu schätzen wissen.

Revisoren und Betrugsermittler

Auch wenn der primäre Fokus diese Buches auf Angriffen auf IT-Systeme zu liegen scheint, ist das Verständnis wichtig, dass die hier beschriebenen Methoden und Verfahren oft auch zum Einsatz kommen, wenn Delikte aus dem Bereich der Wirtschaftskriminalität zu ermitteln sind. Wie der Leser in den späteren Kapiteln schnell merken wird, unterscheidet sich das Vorgehen bei der Sammlung bzw. Analyse von digitalen Spuren nach einem Servereinbruch nicht sonderlich von dem Vorgehen, das nach dem Ausnutzen von Sicherheits- und Konfigurationslücken eines internen Mail- oder Buchführungssystems nötig ist. Benutzt ein gewöhnlicher Straftäter informationstechnische Systeme wie PC, PDA oder Mobiltelefon, müssen auch die dort befindlichen digitalen Spuren gesichert, analysiert und dokumentiert werden.

Technische Voraussetzungen

Um dieses Buch besser zu verstehen, sollte der Leser über ein grundlegendes Verständnis für Basis-Sicherheitstechnologien wie Firewalls, Intrusion-Detection-Systeme und Verschlüsselung verfügen. Das fehlerfreie Bewegen auf der Kommandozeile kann an manchen Stellen den Zugang zu einigen vorgestellten technischen Details erleichtern, ist aber nicht zwingend nötig, um das Grundproblem zu

2. Antwort bzw. Reaktion auf einen (Sicherheits-)Vorfall

verstehen. Ebenso sollten mangelnde Windows-Kenntnisse keinen Leser daran hindern, einen Überblick dafür zu bekommen, welche Möglichkeiten Windows-basierte Tools bieten können.

Im Zweifelsfall Experten hinzuziehen!

Dem Autor ist es wichtig darauf hinzuweisen, dass bei unsachgemäßem Vorgehen evtl. wichtige Beweise vernichtet werden oder das eigene System gänzlich unbrauchbar gemacht werden kann. Im Zweifelsfall sollten hier unbedingt Experten hinzugezogen werden. Wenn man die in diesem Buch besprochenen Tätigkeiten vielleicht nicht selbst durchführen kann, bietet das erworbene Wissen dennoch die Möglichkeit, sich einen Überblick über die verfügbaren Methoden zu verschaffen und die Ergebnisse toolgestützter Untersuchungen besser auf ihre Aussagekraft zu bewerten. Dieses kann hilfreich sein, wenn ein Ermittlungsbericht zu begutachten ist oder die Chancen und Risiken einer möglichen Ermittlung abgewogen werden müssen.

Was lernt man in diesem Buch?

Schwerpunkt: Systemeinbrüche

In diesem Buch werden Teilaspekte des System- oder Computereinbruchs und die Probleme bei deren Ermittlung näher beleuchtet. Die weiterführenden Bereiche der Computerkriminalität – wie Computerbetrug oder Täuschung im Rechtsverkehr beim Einsatz von Datenverarbeitung bzw. Fälschung beweiserheblicher Daten – werden dagegen nur zur Verdeutlichung der Themenrelevanz erwähnt. Dies hat seine Ursache darin, dass sich die Computer-Forensik häufig nur schwer abgrenzen lässt. Die grundlegenden Informationen, die für die juristische Würdigung »klassischer« Vergehen benötigt werden, haben aber auch in der Welt der Computer-Forensik ihre Gültigkeit:

- Wer, Was, Wo, Wann, Womit, Wie und Weshalb

Beweise suchen, erkennen, bewerten

Es geht dabei vorrangig um die Gewinnung von Beweisen, die aussagekräftig genug sind, damit über die nachfolgenden Schritte besonnen entschieden werden kann. Dieses Buch zeigt, wo man nach Beweisen suchen sollte, wie man sie erkennen kann, wie sie zu bewerten sind und wie sie für das Gericht verwertbar gesichert werden sollten.

Was lernt man in diesem Buch nicht?

Keine IT-Grundlagen, keine speziellen Sicherheitstechnologien, keine juristischen Details

Dieses Buch vermittelt weder die wesentlichen Grundlagen zu den Themengebieten der IT-Sicherheit noch vollständige und abschließende Informationen über die Funktionsweise und Wirksamkeit von Firewalls, Intrusion-Detection-Systemen oder anderen Sicherheitstechnologien. Ebenso wird dieses Buch nicht den Ansprüchen eines juristi-

schen Tiefenwerks gerecht werden. Zu allen diesen Gebieten existiert bereits hervorragende Standardliteratur, die diese Themen grundlegend und oft auch abschließend behandelt. Dieses Buch kann nicht alle eventuell infrage kommenden Methoden und Tools in voller Tiefe vorstellen. Aus diesem Grund werden die bisher eher selten vorgestellten Verfahren gezeigt und die bereits bekannten Herangehensweisen, z. B. aus dem breiten Bereich der netzwerkbasierten Intrusion Detection, weiter in den Hintergrund gestellt. An den entsprechenden Stellen werden aber Anregungen für die weitergehende Recherche geliefert.

Einige der in diesem Buch angesprochenen organisatorischen Vorarbeiten lassen sich naturgemäß auch nicht eins zu eins in der eigenen Organisation umsetzen, da sich aus jeder Ermittlungssituation ein unterschiedlicher Handlungsbedarf ergeben kann. Aus diesem Grund eignet sich dieses Buch nur bedingt als vollständige Checkliste. Wie in allen Gebieten der Informationstechnologie ist im Bereich der Computer-Forensik eine stete Fortentwicklung der technischen Möglichkeiten sowohl bei den Tätern als auch bei den Ermittlern zu verzeichnen. Dem Grundsatz »Erwarte das Unerwartete« folgend, kann hier nur ein Überblick über die aktuelle Situation gegeben werden, alle zukünftigen Entwicklungen erfordern womöglich andere Sichtweisen und Ermittlungstechnologien.

Wie liest man dieses Buch?

Detaillierungsgrad

Neben den Möglichkeiten zur Auffindung von Angriffsspuren beschreibt dieses Buch auch, welche technischen und organisatorischen Rahmenbedingungen für eine erfolgreiche Ermittlung unabdingbar sind. Der Detaillierungsgrad nimmt mit jedem weiteren Kapitel zu. Von den einführenden und grundlegenden Beschreibungen geht es über konkrete Prozessabläufe und Ermittlungstechniken hin zu praktischen Beispielen anhand verschiedener Fragestellungen und Spezialaspekte. Ist der Leser neu in der Gesamtthematik, sollte er dieses Buch von vorne nach hinten durchlesen. Bestehen Vorkenntnisse in den einzelnen Gebieten, kann sicherlich das eine oder andere Kapitel quergelesen werden.

Für einzelne Fragestellungen können Sie dieses Buch auch später als Nachschlagewerk bzw. Informationsquelle verwenden. Da die Computertechnologie oft schnellen Veränderungen unterworfen ist und Ermittlungswerkzeuge und -methoden häufig angepasst werden, können Sie weitere aktuelle Informationen zu den vorgestellten Tools auf der Homepage zu diesem Buch unter *http://computer-forensik.org* finden.

Kapitel 1

Risiken und Täter

In diesem Kapitel werden die Bedrohungssituation und die Motivation der Täter näher beleuchtet. Weiterhin findet sich dort eine Einschätzung der Risikoverteilung auf die Netzteilnehmer. Um die Relevanz für die eigene Umgebung besser abschätzen zu können, findet der Leser in diesem Kapitel hilfreiche statistische Aussagen. Deshalb eignet es sich besonders gut als Einstieg in das Thema.

Kapitel 2

Angriffstechniken

Wenn man Angriffsspuren erkennen möchte, muss man wissen, wie ein Angriff abläuft und welche Angriffsmuster überhaupt erkennbare Spuren hinterlassen. Aus diesem Grund werden hier einige Angriffstechniken erklärt. Die Erläuterungen gehen aber nur so weit, wie sie für das Verständnis der folgenden Kapitel nötig sind. Es existieren einige sehr interessante Bücher, die sich mit Angriffstechniken befassen und dies im Einzelnen erklären. Leser, die sich mit Angriffserkennung zum ersten Mal beschäftigen, sollten dieses Kapitel lesen.

Kapitel 3

Incident Response

Die notwendigen organisatorischen Vorarbeiten bei der Behandlung von Sicherheitsvorfällen und grundlegende Informationen über ein sinnvolles Incident-Response-Verfahren sind dem Kapitel 3 zu entnehmen. Dies umfasst sowohl die richtige Auswahl der Personen, die an der Ermittlung beteiligt sind, als auch die richtige Auswahl der Response-Strategie. Es werden alle wichtigen Schritte bei einer Sicherheitsvorfallbehandlung erläutert. Techniker, die den globalen Blick bekommen möchten, finden hier interessante Informationen.

Kapitel 4

Abläufe und Methoden

Kapitel 4 erklärt im Überblick alle wesentlichen Handlungen bei der Ermittlung eines Computereinbruchs mit allen durchzuführenden Tätigkeiten und Hinweisen zur richtigen Sicherung von Beweismitteln. Es werden die wesentlichen und unabdingbaren Schritte und Tätigkeiten erläutert, die nötig sind, um ein System zu analysieren. Hierzu gehören Antworten auf Fragen wie: Was soll ich machen, wenn der Rechner noch läuft? Wo soll zuerst nachgeschaut werden? Wie gehe ich bei einer forensischen Duplikation vor? Welche Untersuchungen können an einem Festplatten-Image durchgeführt werden? Wie gehe ich korrekt mit Beweismitteln um? Und so weiter.

Kapitel 5

Post-mortem-Analyse

Dieses Kapitel widmet sich ausführlich der zentralen Forensik-Technik »Post-mortem-Analyse«. Es werden wesentliche Fragestellungen zur Suche von Beweisspuren auf einem angegriffenen System vorgestellt. Der Leser erfährt, an welchen Stellen er nach Spuren suchen sollte, wie er diese bewerten kann und wie er damit seine Ermittlungsstrategie besser planen kann. Das Lesen dieses Kapitels ist hilfreich, wenn man die Arbeitsweise der später vorgestellten Werkzeuge besser verstehen möchte.

Kapitel 6

Werkzeuge

In diesem Kapitel wird die konkrete Arbeit mit Forensik- und Incident-Response-Werkzeugen erläutert. Die aktuell verfügbaren Toolsammlungen werden vorgestellt und deren Grundfunktion erklärt. Der letzte Teil in diesem Kapitel widmet sich den Möglichkeiten, einen eigenen Werkzeugkasten zusammenzustellen.

Kapitel 7

Analysebeispiele

Die in Kapitel 4 und 5 vorgestellten Vorgehensweisen sowie die Werkzeugsammlungen aus Kapitel 6 werden in diesem Kapitel an konkreten Beispielen illustriert. Anhand von typischen Analyseszenarien wird sowohl auf typische Windows- als auch Unix-Umgebungen eingegangen. Außerdem wird die forensische Analyse bei mobilen Geräten wie PDAs und Mobiltelefonen sowie bei Routern vorgeführt. Der Leser wird schnell erkennen können, welche Werkzeuge sich für welche Untersuchungsumgebung besonders eignen.

Kapitel 8

Empfehlungen für den Schadensfall

In diesem kurzen Kapitel werden in Form eines Best-Practice-Ansatzes wesentliche Empfehlungen für einen bereits eingetretenen Schadensfall vorgestellt. Diese Maßnahmen sind als Basis für die Erstellung individueller Handlungsanweisungen geeignet und sollten an die jeweilige Situation angepasst werden.

Kapitel 9

Backtracing

Kapitel 9 liefert einige Hinweise und Tricks zur Rückverfolgung von möglichen Tatverdächtigen anhand der gefundenen Spuren. Dem Leser wird sehr schnell deutlich werden, wo die Fallstricke liegen,

wenn man z. B. eine IP-Adresse in den Datenspuren gefunden hat und glaubt, damit den Täter zu kennen. Dieses Kapitel kann nur unvollständig sein, bietet aber für die typischen Fundspuren hilfreiche Hinweise.

Kapitel 10

Rechtliche Schritte

Wenn es im Rahmen einer Ermittlung zur Entscheidung über eine weitere juristischen Würdigung kommen sollte, hilft Kapitel 10 weiter, da dort Empfehlungen für den Schadensfall gegeben werden. Neben einigen juristischen Begriffen werden die Vor- und Nachteile der einzuschlagenden juristischen Wege erläutert. Da Ermittlungen eines Sicherheitsvorfalls nicht selten mit der Absicht durchgeführt werden, den Täter strafrechtlich oder zivilrechtlich zur Verantwortung zu ziehen, beschäftigt sich dieses Kapitel mit der Verwertbarkeit von Beweismitteln bei Gericht. Dieses Kapitel wurde mit Unterstützung von Kriminalhauptkommissar Stefan Becker, Sachbearbeiter für Computerkriminalität am Polizeipräsidium Bonn, erstellt.

Was ist neu in der 6. Auflage?

In der 6. Auflage wurden Statistiken und Toolbeschreibungen aktualisiert sowie neueste rechtliche Entwicklungen aufgenommen. Hinzugekommen sind neue Ansätze der strukturierten Untersuchung von Hauptspeicherinhalten und die Analyse von Malware.

Was ist neu in der 5. Auflage?

Vieles ändert sich, so auch Statistiken, Einschätzungen und Versionsnummern. Wenn auch der Kern dieses Buches der gleiche geblieben ist, habe ich einige Erweiterungen und Ergänzungen vorgenommen. Fast alle Kapitel sind überarbeitet und erweitert, so wurden z. B. die Artefakte von Windows 7 (insbesondere der Registry und des Dateisystems) und erweiterte Analysetechniken hinzugefügt. Es sind mittlerweile auch neue Linux-Live-CDs verfügbar, die ebenfalls vorgestellt werden.

Was ist neu in der 4. Auflage?

Die 4. Auflage enthält einige wenige neue Dinge. Selbstverständlich habe ich die Toolübersicht angepasst und neue Werkzeuge aufgenommen. Ebenso sind die Statistiken und auch die juristischen Ausführungen aktualisiert worden.

Was ist neu in der 3. Auflage?

Natürlich wurden einige Statistiken aktualisiert und diejenigen, die nicht mehr gepflegt werden, komplett entfernt. Gerade auf dem Gebiet des Tooleinsatzes hat sich seit der letzten Auflage viel getan und es wurden auch neue Ermittlungstechniken bei der Sammlung und Analyse von flüchtigen Daten eingeführt.

Das Vorgehen bei der Behandlung von Sicherheitsvorfällen unterliegt einer zunehmenden Standardisierung. Dieses Buch trägt dem Rechnung, indem das S-A-P-Modell näher beschrieben sowie die entsprechenden Empfehlungen des BSI aufgenommen wurden.

Die Computer-Forensik ist, im Vergleich zu den anderen forensischen Disziplinen, ein noch recht junges Fachgebiet. Es werden ständig neue Ermittlungsmethoden entwickelt. In dieser Auflage wurden einige davon aufgenommen, wie beispielsweise die neuen Ansätze bei der Analyse von Hauptspeicherkopien.

Viele Leser haben sich noch mehr technische plattformspezifische Details gewünscht. Dieses Buch soll jedoch eine Einführung mit den wesentlichen Ermittlungstechniken liefern. Eine tiefere Beschäftigung mit allen möglichen Plattformspezifika würde daher den Rahmen dieses Buches sprengen. Dennoch beschäftigt sich eine weitere Ergänzung in dieser Auflage mit den Neuerungen, die in Windows Vista und seinem Dateisystem enthalten sind. Es sind viele neue Spuren hinzugekommen, andere – altbewährte – wurden verändert.

Der Bereich der Analyse von PDAs und Mobiltelefonen wurde ebenfalls wesentlich erweitert und an die aktuelle technische Entwicklung angepasst.

Was ist neu in der 2. Auflage?

Neben der Aktualisierung einiger Statistiken und rechtlichen Rahmenbedingungen sind in dieser Auflage die neuen Funktionen der beschriebenen Werkzeuge ergänzt worden. So flossen die Änderungen in EnCase 5 sowie im AccessData FTK 1.60 in diese Ausgabe ein. Da das

ebenfalls beschriebene F.I.R.E. nur noch sporadisch aktualisiert wird, wurde das auf Knoppix basierende Helix als Empfehlung für Ermittler aufgenommen. Ebenfalls neu ist der Abschnitt über das deutsche Werkzeug X-Ways Forensics.