Alexander Geschonneck ist leitender Sicherheitsberater bei der HiSolutions AG in Berlin. Seit 1993 ist er branchenübergreifend im strategischen und operativen IT-Sicherheitsumfeld tätig. Alexander Geschonneck ist Mitautor des IT-Grundschutzhandbuches des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie Autor zahlreicher Publikationen zur Informationssicherheit und Computer-Forensik. Seine Arbeitsgebiete sind u.a. Beratung im Umfeld der Informationssicherheit, Aufbau und Coaching von IT-Sicherheitsmanagementteams, Risiko- und Sicherheitsanalysen, Notfallplanung, Penetrationstests sowie Sicherheitsvorfallsbehandlung.

***iX*-Edition**
In der *iX*-Edition erscheinen Titel, die vom dpunkt.verlag gemeinsam mit der Redaktion der Computerzeitschrift *iX* ausgewählt und konzipiert wurden. Inhaltlicher Schwerpunkt dieser Reihe sind Standardwerke zu professioneller Datenverarbeitung und Internet.

Alexander Geschonneck

Computer-Forensik

Computerstraftaten erkennen, ermitteln, aufklären

3., aktualisierte und erweiterte Auflage

dpunkt.verlag

Alexander Geschonneck
geschonneck@computer-forensik.org

Lektorat: René Schönfeldt
Copy-Editing: Michaela Schneider, Berlin
Herstellung: Birgit Bäuerlein
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: Koninklijke Wöhrmann B.V., Zutphen, Niederlande

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

ISBN 978-3-89864-534-8

3., aktualisierte und erweiterte Auflage 2008

Ringstraße 19 b
69115 Heidelberg

5 4 3 2 1 0

Geleitwort

Ungefähr zehn Jahre ist es jetzt her, dass ich den ersten dieser Anrufe bekam. Damals arbeitete ich im Computer-Notfallteam des Deutschen Forschungsnetzes[1], und regelmäßig riefen uns Administratoren und Entscheider an, die nach einem Angriff auf ihre Systeme nach Hilfe suchten. Hilferufe waren also nichts Neues für mich, doch dieser Anruf war anders ... okay, Rechner waren kompromittiert worden, aber diesmal handelte es sich wohl um einen Innentäter. Und die Organisation wollte nicht nur einfach die Sicherheitslücken schließen und zum Alltagsbetrieb übergehen, sondern sie wollte ganz genau wissen, was mit den Rechnern passiert war, auf denen der Vorstand vertrauliche Dokumente abzulegen pflegte.

Damals gab es noch keine Computer-Forensik und die ersten Standardvorgehensweisen waren gerade mal in ein paar internen Dokumenten staatlicher Ermittlungsbehörden festgehalten. Dennoch leisteten die technischen Experten bereits gute Arbeit. Was jedoch bedeutet »gut« in diesem Kontext? Technische Experten an technische Probleme zu setzen liefert in der Regel die Antwort auf die Frage: »Was ist passiert?« ... und so erhielt auch das oben angesprochene Unternehmen seine Antworten ...

Mir ist nicht bekannt, ob das Unternehmen versuchte, vor Gericht Recht zu bekommen. Doch fielen viele Organisationen, die dies damals versuchten, vor Gericht schlicht und einfach durch. Während für die Techniker alles klar war, hatten sie in den Augen des Gerichts und der mit den Verfahren dort vertrauten Fachleute von Anfang an alles falsch gemacht: »Und wo war die Festplatte gelagert worden, bis Sie Zeit hatten, eine genaue Untersuchung vorzunehmen?« – »Ah so, im Safe? Wer hatte dazu Zugang?« – »Wie, das ganze Netzwerkteam? Sieben Leute?«

1. DFN-CERT; http://www.cert.dfn.de/

Es brauchte Ereignisse wie diese, um den Weg zu ebnen. Wie so oft ist eben nicht die Technik das Problem, sondern die Einbettung in den gesellschaftlichen Kontext. Wir Techniker kümmerten uns also mehr um das »Wie mache ich das?« bei der Beweissicherung als um das »Wie hat der Angreifer das gemacht?« – Aber auch die anderen an dieser Thematik interessierten Fachleute halfen mit, nicht nur ein Problembewusstsein, sondern auch angemessene Lösungen zu entwickeln, indem sie teilweise bereits lang erprobte Herangehensweisen auf ein neues Anwendungsgebiet übertrugen. Schließlich war es nur eine Frage der Zeit, bis auch eine treffende Bezeichnung für das neue, sich langsam entwickelnde Fachgebiet der IT-Sicherheit aufkam: »Computer-Forensik«.

Während sich mehr und mehr herauskristallisiert, was alles »dazu gehört«, gibt es schon wieder Spezialthemen, z.B. die »Disk-Forensik« oder die »Network-Forensik«, und in naher Zukunft wird es wohl auch Experten geben, die sich mit »Nano-Forensik« beschäftigen müssen. Mit den Veränderungen der Systeme, Anwendungen und Nutzungen moderner Computer und Netzwerke ändert sich das technische Wissen, das ein Spezialist beherrschen muss. Aber all diese Dynamik und die technischen Details – mögen sie auch noch so interessant sein – dürfen nicht von dem elementaren Kernpunkt ablenken, den auch dieses Buch herausstellt und zu dem es immer wieder zurückkehrt, dem Mantra eines Forensikers: Planen – Beweise sichern – Beweise schützen – Untersuchen – Bewerten – Dokumentieren.

Überhaupt kann der Wert einer guten Vorbereitung und Planung nicht hoch genug eingeschätzt werden. Dies gilt nicht nur für die Forensik selbst, sondern für alle Aspekte der IT-Sicherheit, vom Sicherheitsmanagement über die Bewältigung von Angriffen und Vorfällen – besser bekannt als Incident Response – bis hin zum Risikomanagement. Und jeder Verantwortliche tut gut daran, bereits hierbei die Forensik mit zu integrieren und die notwendigen Voraussetzungen für eine später schnelle und effektive Beweissicherung zu schaffen.

Wie auch dieses Buch herausarbeitet, ist die Computer-Forensik dabei das Bindeglied zwischen der Incident Response, die ja verstärkt auf die Bewältigung der Folgen und Schäden ausgerichtet ist, und einer erfolgreichen Strafverfolgung bzw. die Erlangung eines Schadensersatzes. Selbst wenn eine gerichtliche Verwertung nicht im Vordergrund steht, schafft erst die detaillierte Analyse die notwendigen Einsichten, warum etwas passieren konnte und wie dies technisch ablief – kritische Details für die notwendige Beseitigung der Mängel. Hier gibt es also eine starke Überlappung mit der Incident Response, die die gleichen Fragen beantworten muss. Oft kann auch erst nach einer Analyse ent-

schieden werden, wie in Bezug auf eine gerichtliche Verwertung weiter vorgegangen werden soll, dann aber müssen alle bis dahin vorgenommenen Schritte bereits einwandfrei durchgeführt und dokumentiert worden sein, ansonsten ist der Fall bereits zu diesem Zeitpunkt verloren.

Nicht verschwiegen werden soll – später wird hierüber mehr zu lesen sein –, dass es auch Zielkonflikte zwischen Incident Response und Forensik gibt: Während die einen Systeme möglichst schnell wieder zum Laufen bekommen möchten, benötigen die anderen einfach eine bestimmte Zeit, die Beweise zu sichern und vor Veränderungen zu schützen. Dies betont noch einmal die Wichtigkeit, solche Konflikte bereits bei der Planung zu berücksichtigen, eventuell Redundanzen zu schaffen, aber in jedem Fall klare Richtlinien festzulegen, nach welchen Prioritäten vorzugehen ist. So gesehen müssen sich sowohl die Incident Response als auch die Computer-Forensik einem ganzheitlichen Sicherheitsverständnis unterordnen, nur dann werden beide ein wirksames Werkzeug des Sicherheitsmanagements.

Abschließend geht dieses Buch kurz auf einen komplexen Aspekt ein, der auch in der Praxis für einige Leser relevant werden könnte, und das ist das Gerichtsverfahren selbst. Denn im Fall der Fälle ist erst danach die Arbeit eines Forensikers wirklich zu Ende. So gut seine vorherige Arbeit auch gewesen sein mag, vor Gericht muss er sie nach bestem Wissen und Gewissen verteidigen. Und das kann sie – oder er – nur, wenn sauber gemäß des Mantras gearbeitet wurde. Ganz klar, dass es vor Gericht auch auf andere Eigenschaften ankommt, z. B. Auftreten und Ausstrahlung, aber das sind Themen, die mit Recht ausgespart wurden, jedoch in der Praxis nicht vernachlässigt werden dürfen.

Schließlich möchte ich noch eine Lanze brechen für mehr Offenheit, so wie es Alexander Geschonneck tut. Nur wenn über Angriffe und Vorfälle nicht immer wieder der Mantel des Schweigens gebreitet wird, können wir als Gesellschaft lernen, wie ernst es wirklich um uns und unsere Sicherheit steht. Klar müssen wir als Berater beide der Wahrheit ins Auge sehen, dass es geradezu schädigend für das *eine* Unternehmen ist, wenn nur dieses allein offen über Vorfälle spricht, auf der anderen Seite können wir nicht so tun, als ob nichts passiert ...

Bleibt mir noch, Alexander Geschonneck zu danken, dass er sich dieser Thematik angenommen hat und es geschafft hat, ein so informatives Buch vorzulegen, das zudem auch auf Aspekte eingeht, die man sonst in ähnlichen Fachbüchern vergebens sucht: die deutsche Sicht der Gesetzgebung und der rechtlichen Rahmenbedingungen.

Ich wünsche Ihnen, dass Sie dieses Buch nie wirklich anwenden müssen, empfehle Ihnen aber dennoch, sich mit den Konzepten, Werkzeugen und Verhaltensweisen zu beschäftigen, bevor es soweit ist!

Klaus-Peter Kossakowski[2]

2. Dr. Klaus-Peter Kossakowski baute 1992 das erste CERT in Deutschland auf. Seit dieser Zeit konzentriert sich seine Arbeit, zunächst als Berater, inzwischen als Geschäftsführer eines Beratungsunternehmens, auf alle Aspekte der praktischen IT-Sicherheit. Klaus-Peter Kossakowski wirkte als Co-Chair der IETF-Arbeitsgruppe GRIP (Guidelines and Recommendations for Incident Processing) und ist seit 1997 gewähltes Mitglied im Steering Committee des Dachverbands internationaler Computer-Notfallteams, FIRST. Seit Juni 2003 hat er dessen Vorsitz inne.