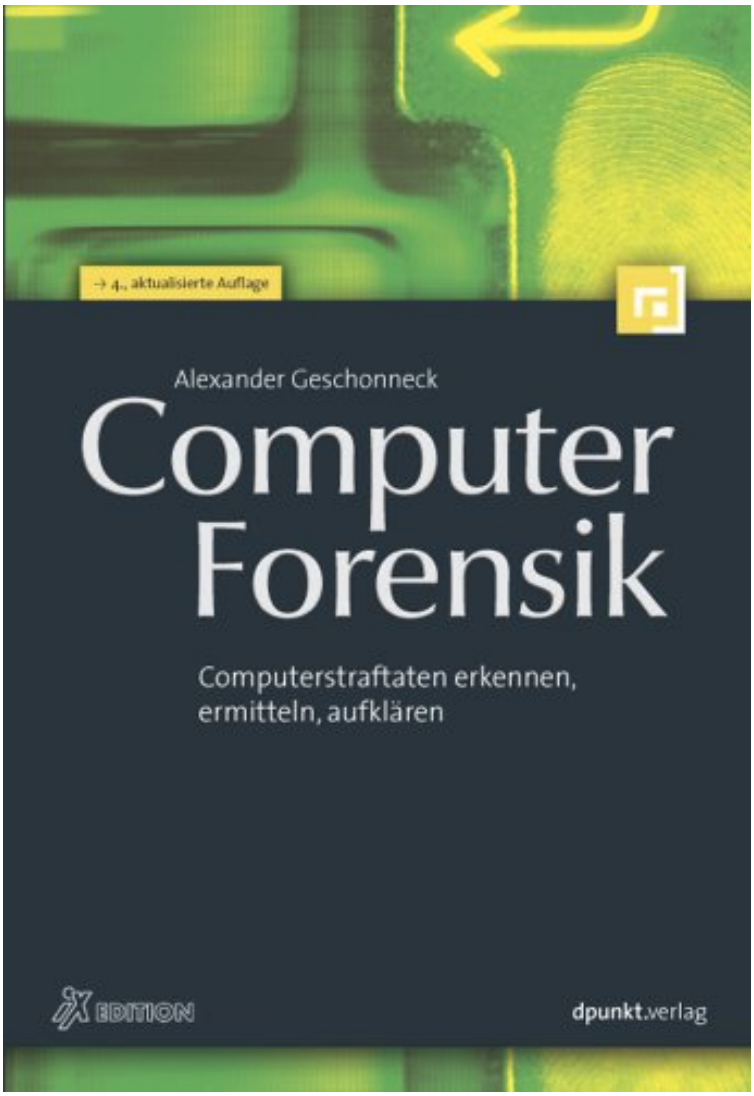
Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklren

Von Alexander Geschonneck
*audiobook | *ebooks | Download PDF | ePub | DOC*



Produktinformation -Verkaufsrang: #1153651 in BcherVerffentlicht am: 2010-02-22Abmessungen: 9.53 x .98b x 6.54l, Einband: Broschiert342 Seiten | File size: 18.Mb

Von Alexander Geschonneck : Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklren before purchasing it in order to gage whether or not it would be worth my time, and all praised Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklren:

KundenrezensionenHilfreichste Kundenrezensionen2 von 2 Kunden fanden die folgende Rezension hilfreich. Ausgezeichnetes und aktuelles KompendiumVon mmDer Autor praesentiert nicht nur Grundlagen sondern auch Hintergruende der Forensik und IT-Sicherheit anschaulich, verstaendlich und in der fuer ihn ueblichen erstklassigen

Qualitaet. (Ich durfte wiederholt in Projekten und unternehmensinternen Runden zur IT Security mit Herrn Geschonneck als Consultant zusammenarbeiten und war stets von seinen Kenntnissen, Praesentationen und seinem gesamten Ansatz begeistert!). Seine hochkaraetigen Kenntnisse spiegeln isch auch in diesem Buch wider und sind damit jedem Interessierten zugaenglich.Wer hier als Hacker technische Detail-Anleitungen sucht oder Methoden zur Abwehr von Cracking quasi "an der Front" vermissen sollte, dem seien stattdessen andere Literatur auf der mehr "handwerklichen" unteren Ebene der Fallenstellerei sowie Anleitungen zu den gaengigen Hard core tools in der Netzwerksicherheit o dgl mehr empfohlen.Fuer die Praxis hilfreich sind ueberdies die Abschnitte zum rechtlichen Umfeld, Fragen der Beweissicherung, Praesentation von forensischen Daten und Unterlagen: unter anderem auch dank der auf dieser Grundlage gewonnenen und in Rechtsstreiten vorgelegten Beweise konnten wir erfolgreich in gerichtlichen und auergerichtlichen Verfahren vorgehen (zB gegen Comment spammers auf unseren Unternehmensseiten). Die erfolgreiche juristische Durchsetzbarkeit unserer Ansprueche u a auch mit Hilfe des in diesem Buch erworbenen Zusatzwissens zeigt, da das Buch auch "fuers wirkliche Leben" geeignet ist.Mindestens SECHS STERNE (wenn es sie denn gaebe)...!23 von 28 Kunden fanden die folgende Rezension hilfreich. Praxisnah und hilfreich. Sehr zu empfehlen!Von Reni GrosserDer Autor versteht es, nicht nur die technischen Spezialisten zu bannen, sondern auch den Einsteigern in dieser Thematik wesentliche Grundlagen zur Ermittlung von Sicherheitsvorfllen zu vermitteln. Der im Vorwort beschriebene Lesepfad ist dafr sehr hilfreich. Neben den vielen technischen Detailinformationen zu Ermittlungsmethoden und Werkzeugen wird auch auf die ebenso ntigen - im Vorfeld zu klrenden - organisatorischen Rahmenbedingungen eingegangen. Im Gegensatz zu den bereits unzhlig auf dem Markt verfgbaren Intrusion Detection Bchern, befasst sich dieses Buch mit der konkreten Ermittlung NACH Entdeckung des Vorfalls: Angefangen von der Spurensuche, ber die gerichtsverwertbare Sicherung von Beweisspuren bis hin zum richtigen Formulieren einer Strafanzeige.Der Autor widmet sich der wesentlichen Frage: wo muss nach Spuren gesucht werden und wie knnen diese richtig gesichert werden. Das Buch ist in dieser Form einzigartig auf dem deutschen Markt, da auch wichtige und hilfreiche Hinweise zur Rechtslage in Deutschland gegeben werden.Ein sehr angehmer Aspekt ist, dass die Ermittlung von Systemeinbrchen an bzw. mit Windows- UND Unix-Systemen beschrieben wird. Ein Kapitel widmet sich auch der Beweissicherung von aktiven Netzkomponenten und von PDAs. Als Ermittler kann man sich eben das Betriebssystem des zu untersuchenden Rechners nicht aussuchen.Ein Kapitel ist durch die Mitarbeit eines kriminalpolizeilichen Ermittlers entstanden. Die Tipps und Empfehlungen, die hier dem Administrator, Sicherheitsbeauftragten oder auch Sicherheitsberater gegeben werden, sind klar, przise und auch fr den juristischem Laien nachvollziehbar.Ein weiterer Tipp ist auch die Website zum Buch, da sich dort aktuelle Informationen zu allen im Buch vorgestellten Werkzeugen befinden.0 von 0 Kunden fanden die folgende Rezension hilfreich. Praxisnaher Einstig in das abstrakte ThemaVon Tom SaharaEinen Revisor muss das Thema Computer Forensik interessieren - auch wenn die Informations- und Kommunikationstechnologie nicht sein Steckenpferd ist. Hat man sich aber zu einem Blick in das Werk durchgerungen, erhlt man hilfreiche Informationen ber die Mglichkeiten der Computer-Forensik.Mit dem enormen Praxis-Bezug bei der Aufklrung von Sicherheitsvorfllen bietet das Buch einen prima Handlungsleitfaden. Gleichzeitig nutzen die Infos der Revision bei Prfungsplanung und Prfung und der IT auch bei der Prophylaxe vor Schadensfllen.Ist es zu einem Schadenfall gekommen wrde ich persnlich - trotz der Literatur - zgern, mich ohne zustzliche fachmnnische Untersttzung an eine Untersuchung zu wagen. Die dazu notwendigen Kenntnisse allein aus dem Werk zu erhalten, verspricht mir der Autor aber auch gar nicht. Er sagt mir aber sehr wohl, was ich berhaupt tun muss, welche Kenntnisse und Methoden bei der Untersuchung von Sicherheitsvorfllen notwendig sind. Und er sagt mir auch, welche Fehler ich dabei machen kann.Die Website zum Buch erachte ich als hilfreichen Zusatznutzen.

.deComputer-Forensik ist das Bindeglied zwischen der Incident Response, der Bewltigung der Folgen und Schden eines Vorfalls oder Angriffs, und einer erfolgreichen Strafverfolgung/eines Schadensersatzes: wie waren/sind die technischen Vorgnge, welche Form von Straftat liegt vor, warum konnte es passieren -- Aufklrung, Feststellung und zuknftige Prvention. Mit Computer-Forensik Systemeinbrche erkennen, ermitteln, aufklren definiert und fokussiert Geschonneck die Ziele und die Arbeit eines IT-Forensikers verstndlich mit Hintergrund, Praxisanwendung und Beispielen. Laut Geschonneck lautet das Mantra eines Forensikers: "Planen -- Beweise sichern -- Beweise schtzen -- Untersuchen -- Bewerten -- Dokumentieren." Wichtig ist dabei ein ganzheitliches Sicherheitsverstndnis schon in der Planung, denn whrend etwa die Incident Response eine mglichst schnelle Wiederherstellung arbeitsfhiger Systeme anstrebt, bentigt die Forensik Zeit, Spuren zu sichern. Das Feld der IT-Sicherheit ist weit und man kann sich ihm aus der Perspektive eines technischen und sozialen Hintergrunds, wie etwa Bruce Schneier in seinem Klassiker Secrets Lies IT-Sicherheit in einer vernetzten Welt oder speziell auf der technisch, konkreten Ebene wie etwa Jrg Fritsch und Steffen Gundel mit Firewalls im Unternehmenseinsatz Grundlagen, Betrieb und Produkte annhern. Geschonneck wendet sich an Administratoren, Sicherheits- und Systemverantwortliche bis hin zu Strafverfolgern und Ermittlern -- dass betrifft sowohl Unternehmen, aber auch Privatpersonen, die mit der Problematik von Systemeinbrchen oder

Datenspionage/- klau konfrontiert werden. Als Grundlage sollte der Leser ber gute Kenntnisse zu Firewalls, Intrusion-Detection-Systeme und Verschlsselung verfgen. Computer-Forensik Systemeinbrche erkennen, ermitteln, aufklren ist das deutsche Standardwerk mit der deutsche Sicht der Gesetzgebung und Rahmenbedingungen zum Wer, Was, Wo, Wann, Womit, Wie und Weshalb. Fundierte bersicht ber mgliche Techniken, Tter und Vorgehensweisen. Theorie, Praxis, Beispiele und Einsicht. Unverzichtbar fr den deutschsprachigen Ersteinstieg ins Thema! --Wolfgang Tretextico.deMit Wissen kann man Macht ausben, man kann verstehen, kontrollieren untersttzen und verhindern - Alexander Geschonneck liefert das Know-how um Wissen zu sammeln, Wissen um die Mglichkeiten, Vorgehensweisen und Ziele von unberechtigten Computerzugriffen - Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklren ist auch in der 4., aktualisierten und berarbeiteten Auflage das Handbuch fr den IT-Sherlock Holmes, aber auch fr Entscheider und Neugierige. Konzentriert arbeitet sich Geschonneck durch die verschiedenen Stadien eines "Vorfalls": Wie sieht die Bedrohungssituation aus, wie luft ein Angriff ab (mit Beispiel) - zentral natrlich der Einstieg in die Computerforensik: Vorgehensweisen, Werkzeuge, Erfahrungen und Ablufe, Rckverfolgung und Tipps fr den Schadensfall. Geschonneck Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklren hat fr den praktischen Einsatz auf einem hohen Admin-Level geschrieben - dennoch knnen auch Entscheider und Themeninteressierte mhelos von den vorgestellten Szenarien und Ablufen profitieren. Ein Standardwerk ohne groe Konkurrenz. --Wolfgang Tre/textico.deKurzbeschreibungUnternehmen, Organisationen und Behrden schtzen ihre IT-Systeme mit umfangreichen Sicherheitsmanahmen. Trotzdem werden diese Systeme immer wieder fr kriminelle Zwecke missbraucht bzw. von Hackern angegriffen. Nach solchen Vorfllen will man erfahren, wie es dazu kam, wie folgenreich der Einbruch ist, wer der beltter war und wie man ihn zur Verantwortung ziehen kann. Dafr bedient man sich der Computer-Forensik. Dieses Buch gibt einen berblick darber, wie man bei der computerforensischen Arbeit vorgeht sowohl im Fall der Flle als auch bei den Vorbereitungen auf mgliche Angriffe bzw. Computerstraftaten. Ausfhrlich und anhand zahlreicher Beispiele wird gezeigt, welche Werkzeuge und Methoden zur Verfgung stehen und wie man sie effizient einsetzt. Der Leser lernt dadurch praxisnah wo man nach Beweisspuren suchen sollte wie man sie erkennen kann wie sie zu bewerten sind wie sie gerichtsverwertbar gesichert werden Ein eigenes Kapitel befasst sich mit der Rolle des privaten Ermittlers, beschreibt die Zusammenarbeit mit den Ermittlungsbehrden und erlutert die Mglichkeiten der zivil- und strafrechtlichen Verfolgung in Deutschland. Fr die 4. Auflage wurde das Buch komplett durchgesehen und aktualisiert.Stimmen zur Vorauflage:'... das Standardwerk zur Computer-Forensik...' c't'Eine Pflichtlektre fr IT-Verantwortliche, Geschftsfhrer und Administratoren.'pcwelt.de