



Datenforensik

Richtlinien, Vorgehensweise bei der Untersuchung

Gerrit Kalkbrenner



Gliederung

- Datenforensik
- Motivation für Computerkriminalität
- Beispiele
- Forensische Analyse



Schlagzeilen

- Polizei warnt vor gefälschten E-Mails mit Trojaner im Anhang

Die Polizei warnt Internet-Nutzer vor E-Mails, die derzeit verschickt werden und mit einem Trojaner verseucht sind.



Welche Arbeiten hängen mit der Schlagzeile zusammen?

- erkennen, dass eine Straftat vorliegt
- ermitteln, wer der Straftäter ist
- -> Datenforensik
- IT-Forensik, Computer-Forensik, digitale Forensik



Forensik

- Unter dem Begriff **Forensik** werden die Arbeitsgebiete zusammengefasst, in denen systematisch kriminelle Handlungen analysiert und identifiziert sowie rekonstruiert bzw. ausgeschlossen werden.



Datenforensik

- Untersuchung von verdächtigen Vorfällen in Zusammenhang mit IT-Systemen
- Tatbestand und Täter
- Erfassung, Analyse und Auswertung digitaler Spuren



„herkömmliche“ Verbrechen (Auszug)

- Erpressung
- Beleidigung
- Geheimnisverrat
- Betrug
- Bilanzfälschung
- Urheberrechtsverletzung
- Verbreitung von kinderpornographischen und verfassungsfeindlichen Inhalten



Datenforensik

Nicht mehr wegzudenken in Zusammenhang mit
„herkömmlichen“ Verbrechen

- zum Zwecke der Steuerfahndung
- computerbezogene Verbrechen
(Netz/Server-Einbrüche)
spielen (noch) eine untergeordnete Rolle.

Computerkriminalität





Computerkriminalität

- Computer-Betrug
- Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten
- Betrug mit Konto- oder EC-Karten mit PIN
- private Softwarepiraterie
- gewerbsmäßige Softwarepiraterie
- Datenveränderung und Computersabotage
- Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung
- Ausspähung von Daten



Computerkriminalität im eigentlichen Sinne

§202 a StGB	Ausspähen von Daten
§202 b StGB	Abfangen von Daten
§202 c StGB	Vorbereiten des Ausspähen Abfangen von Daten
§263 a StGB	Computerbetrug
§269 StGB	Fälschung beweiserheblicher Daten
§270 StGB	Täuschung im Rechtsverkehr bei Datenverarbeitung
§271, §274 Abs. 1 Nr. 2, §348 StGB	Falschbeurkundung/Urkundenunterdrückung im Zusammenhang mit Datenverarbeitung
§303 a StGB	Datenveränderung
§303 b StGB	Computersabotage



Motivation für Computerkriminalität

- soziale Motivation
- technische Motivation
- politische Motivation
- finanzielle Motivation
- staatlich-politische Motivation



Hacker und Script Kiddies

- Weltweit sind lediglich 500 bis 1000 Hacker dazu in der Lage Sicherheitslücken zu finden
- 5000 Hacker können Programme schreiben, die Sicherheitslücken nutzen
- 100 000 Script Kiddies nutzen vorbereitete Werkzeuge für den Systemeinbruch



Innentäter, Außentäter

- Angriffe durch Mitarbeiter
 - Rache
 - Bereicherung
 - Verschleierung
 - Nutzen Insider Information
- Angriffe durch fremde Personen
 - nutzen Schwachstellen
 - Spionage

Beispiel 1: Hacker aus Hannover (Ende 1980er J.)

- erste spektakuläre Jagd auf den Hacker Markus Hess, der aus Hannover in Militärcomputer in den USA einbricht
- Clifford Stoll vom Lawrence Berkeley National Laboratory
- umfangreich eingespeiste Dokumente
- Telefon Fangschaltung



Beispiel 2:

W32.Lovsan/ MSBlast und Stromausfall in NY

- Computerwurm
- sollte am 16. August 2003 einen Distributed-Denial-of-Service-Angriff auf die Updateseiten der Firma Microsoft durchführen
- 14. August 2003, Stromausfall in NY/USA

Beispiel 3: Datenmanipulation

- ein Mitarbeiter verschafft sich (unerlaubt) Zugang zu einem Informationssystem
- entnimmt wichtige Information, oder
- manipuliert Information
- eigenes Vorhaben / eigene Firma
- Vertuschung von Fehlern/ Vorteilnahme



Datenforensik

- Ermittlung: Tatbestand und Täter
- Beschlagnahmung der IT
- Untersuchung der Vorfälle
- Überführung der Täter

Beweismittelsicherung

im Vorfeld sind folgende Dinge zu beachten:

- originale Beweismaterial so wenig wie möglich „bewegen“
Jede „Bewegung“ des Beweismaterials kann eine Verfälschung zur Folge haben
- Beweismittelkette ist von zentraler Bedeutung
- erfordert eine lückenlose Dokumentation
- persönliches Wissen darf nie überschätzt werden!
- Einbeziehung verschiedener Fachleute zu Spezialthemen (zum Beispiel Datenrettung) ist in Erwägung zu ziehen.

Tätigkeiten in der Forensik

Durchführung einer Analyse mittels Datenforensik erfolgt in einem festgelegten Prozess:

- Identifizierung
 - Sicherstellung
 - Analyse
 - Präsentation / Aufbereitung
-
- S – A – P: Secure, Analyse, Present



Wer - Wann - Warum - Was - Wann - Wie

- ‚Wer‘ – Wer bewegte bzw. veränderte Daten? Wer war anwesend und beteiligt?
- ‚Wann‘ – Datum und Uhrzeit.
- ‚Warum‘ – Warum wurde eine Änderung, Bewegung und/oder Abweichung vorgenommen?
- ‚Wo‘ – Genaue Ortsangabe.
- ‚Was‘ – Was wurde genau getan?
- ‚Wie‘ – Wie wurde vorgegangen bzw. welche Tools und/oder welche physikalischen Mittel wurden eingesetzt?



Incident Response

- Reaktion auf Systemeinträge in Firmen
- Ergründung des Vorfalles
- Dokumentation
- Reparatur
- Gegenmaßnahmen

Incident Response und Forensik

- Bezüglich der Untersuchung des Vorfalles werden gleiche Ziele verfolgt

Aber:

- Incident Response:
 - Wiederherstellung des Betriebes
 - Verhinderung zukünftiger Einbrüche
- Forensik:
 - Überführung der Täter

Incident Response Team

- Ziel ist rasche Wiederherstellung des regulären Betriebs
- nicht eingespielte Security Patches
- Fehler in der Sicherheitskonfiguration
- Mitarbeiter holen dieses gerne schnell nach
- technische Mitarbeiter aus den Rechenzentren verschleiern gerne eigene Fehler
- Furcht vor Abstrafung, wenn kein Täter ermittelt wird

Beweismittelsicherung

- um Beweise zu sichern, werden Datenträger sowie Protokolle des Netzverkehrs gesichert und analysiert
- für die Analyse von Datenträgern wird in der Regel vorher ein "forensisches Duplikat" erstellt
- eine Reihenfolge der Sicherung der digitalen Spuren ist festzulegen



Alexander Geschonnek

1

Spurensicherung: problematisch

1. ersten Schritt: das Ziehen des Netzsteckers des PC
 2. Ausbau der Festplatten
 3. Kopie auf eine mitgebrachte Sicherungsplatte
- schließt die Untersuchung des Arbeitsspeicherinhaltes aus
 - gefährdet bei einigen Dateisystemen die Datensicherheit
 - moderne Dateisysteme behalten viele relevante Daten im Speicher, diese gehen verloren
 - Probleme können nur noch teilweise durch Selbstreparaturmaßnahmen des Dateisystems wieder korrigiert werden

Fortgeschrittene Spionagesoftware

- in professionellen Angriffen kommt Spionagesoftware zum Einsatz, die sich ausschließlich im Hauptspeicher des Zielsystems einnistet und keine Spuren auf der Festplatte hinterlässt
- Analyse flüchtiger Daten: Live Response
- Helix/Knoppix: statisch kompilierte System-Binaries (bash, .. , ifconfig)
- Ausgabe aller wichtigen Informationen eines laufenden Linux-Systems
- Sicherung auf einem externen Datenträger oder Netz

Sichern vor dem Abschalten (steht im Ram):

- Welche Benutzer waren zu diesem Zeitpunkt angemeldet?
- Welche Prozesse waren tatsächlich aktiv und was stand in deren Speicherbereichen?
- Zu welchen Systemen existierten Netzwerkverbindungen?



Weiteres Material für die Forensik

- PC- und Serversysteme
- klassische Datenträgeranalyse von Festplatten
- immer wichtiger: digitaler Spuren auf Smartphones
- Zugriff auf Smartphones ohne PW?



Vorgehensweise bei der Untersuchung

1. Identifizierung einer Straftat
2. Sicherstellung der Beweise
3. Forensische Analyse
4. Präsentation / Aufbereitung



1. Identifizierung einer Straftat

- möglichst genauen Dokumentation der vorgefundenen Situation
- Bestandsaufnahme des eigentlichen Sicherheitsvorfalles
- Welche Beweise sind zugänglich?
- geben Log-Dateien Auskunft?
- festhalten, wo und wie diese Beweise vorrätig sind
- Umgebungen, in denen die Beweismittel vorliegen (z. B. Betriebssysteme, Dateisysteme)



2. Sicherstellung der Beweise

- Integrität der digitalen Beweise und der Beweiskette
- Auswahl der richtigen Mittel zur Sicherung der Beweise
- Im Regelfall Sichern von Beweisen auf Datenträgern.
- Nutzung von Medien, die einmalig beschreibbar sind.
- Gewährleistung der Unversehrtheit von Daten
- Hash-Werte / Prüfsummen



3. Forensische Analyse

- erfordert Wissen über Netzwerktopologien, Anwendungen, und aktuelle System-Verwundbarkeiten
- sehr hoher Grad an Improvisationsvermögen
- Hinzuziehen externer Fachleute
- benötigtes Wissen geht weit über Administrator-Kenntnisse hinaus
- betriebssystemnahe Programmierkenntnisse

- Zweck der Analyse liegt in der Veranschaulichung und Untersuchung der Beweise
- richtige Deutung der Tatsachen
- Bemessung der Ursachen des Vorfalles und der Wirkungsweise des eingetretenen Vorfalls
- Analyse findet typischerweise nicht am originären System statt

4. Aufbereitung und Präsentation

- Aufbereiten der Analyse in Form eines Berichtes
- grundsätzliche Motivation der Untersuchung
- Ermittlung der Identität des Täters / der Täter,
- Ermittlung des Zeitraums der Tat (Erstellung „Timeline“),
- Ermittlung des Umfangs der Tat,
- Ermittlung der Motivation der Tat und
- Ermittlung der Ursache und Durchführung
- Nicht alle Punkte lassen sich restlos klären, es hängt vom vorhandenen Beweismaterial / Qualität der Analyse ab.



Präsentation vor Gericht

- Beweismittelkette ist von zentraler Bedeutung
- lückenlose Dokumentation
- Ausschluss von andern Ursachen
- Nachweis, dass Beweise nicht manipuliert wurden (Hash-Werte)



Zusammenfassung

- viele IT- und Beratungsfirmen bieten forensische Untersuchungen als Dienstleistung an
- auch polizeiliche Behörden beschäftigen zunehmend mehr Fachkräfte in diesem Bereich
- Aufbau eines Zentrums für Datenforensik und IT-Sicherheit
- Beratung / Forschung



Literatur

- Alexander Geschonneck: "Computer-Forensik: Computerstraftaten erkennen, ermitteln, aufklären", Dpunkt Verlag, 2008
- Alexander Geschonneck: "Computer-Forensik. Systemeinträge erkennen, ermitteln, aufklären, Dpunkt Verlag, 2006
- Karl-Werner Jäger: Begutachtung und rechtliche Bewertung von EDV-Mängeln, 2003
- Kevin Mandia, Chris Prosise, Mat Pepe: "Incident Response & Computer Forensics" McGraw Hill, 2003, ISBN 007222696X
- Dan Farmer, Wietse Venema: "Forensic Discovery", Addison Wesley, 2006, ISBN 0-201-63497-X Holger Reibold: Digitale Forensik mit Helix: Helix kompakt, Bomots Verlag, 2008)
- Erich Wulff: Das Unglück der kleinen Giftmischerin. Und zehn weitere Geschichten aus der Forensik, Balance Buch + Medien, 2007
- Clifford Stoll: Kuckucksei. Die Jagd auf die deutschen Hacker, die das Pentagon knackten. Fischer Verlag, Frankfurt/M. 2001, ISBN 3-596-13984-8





Cybercrime-Konvention (ETS-No.: 185)

- Die europäische heißt mit offiziellem Titel: "Convention on Cybercrime (Convention sur la cybercriminalite)". ETS steht für *European Treaties Series*. Die Konvention wurde am 8. November 2001 durch das Ministerkomitee des Europarats in Budapest verabschiedet. Am 23. November haben die ersten Staaten die Cybercrime-Konvention (ETS-No.: 185) unterzeichnet. Zu diesen 45 Staaten gehören viele Mitgliedsstaaten der Europäischen Union, Schweiz, Ukraine, Rumänien sowie nicht-europäische Staaten wie Japan, Kanada, Südafrika und die Vereinigten Staaten von Amerika.
- Das Ziel der Cybercrime-Konvention ist die Bereitstellung von Gesetzen und Vorgehensweisen zur Bekämpfung "verschiedener Arten kriminellen Verhaltens gegen Computer Systeme, Netzwerke und Daten". Die europäische Cybercrime-Konvention steht online unter der folgenden Adresse zur Verfügung:
- <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>



Cybercrime

- Ein Zusatzprotokoll zur Konvention über Computerkriminalität wurde Januar 2003 zur Zeichnung aufgelegt. Es fordert die Staaten auf, die Verbreitung von fremdenfeindlichem und rassistischem Material über Computersysteme zu einem Straftatbestand zu erheben.
- Das Cybercrime-Abkommen sieht erweiterte Befugnisse zum Abhören der Internetkommunikation und zum grenzüberschreitenden Datenaustausch vor. Internetkommunikation soll in Echtzeit abgehört werden können, und es müssen Vorkehrungen getroffen werden, die Verkehrsdaten zu speichern. Neben der strafrechtlichen Einordnung von illegalem Abhören, dem Eindringen und Stören von Computersystemen, dem Stehlen, Manipulieren oder Löschen von Daten stellt das Abkommen auch Vergehen gegen das Copyright, das Umgehen von Kopierschutzsystemen, das Herstellen, Verbreiten und Verfügbarmachen von Kinderpornografie sowie Verbrechen, die unter Ausnutzung von Computer-Netzwerken begangen werden können (Betrug, Geldwäsche, Vorbereitung terroristischer Akte), unter Strafe [10].
- Die Konvention ist am 1.7.2004 in Kraft getreten und ist von den Mitgliedstaaten in staatliches Recht umzusetzen.