Computer Forensik

Systemeinbrüche ermitteln und aufklären

Alexander Geschonneck, HiSolutions AG, Berlin

GUUG Frühjahrsfachgespräche 2004

Agenda

- Einführung
- Tätereinschätzung
- Ermittlungsstrategien
- Fundorte für Beweisspuren
- Häufige Fehler

Was ist Computer Forensik?

Computer-Forensik[1] (oder auch Digitale Forensik):

> Nachweis und die Ermittlung von Straftaten im Bereich der Computerkriminalität

> Nachweis und Aufklärung von strafbaren Handlungen z. B. durch Analyse von digitalen Spuren

Kriminalistische Fragestellungen:

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

Ziel der Ermittlung

> Erkennen der Methode oder der Schwachstelle, die zum Systemeinbruch geführt haben könnte,

> Ermittlung des entstanden Schadens nach einem Systemeinbruch,

> Identifikation des Angreifers,

> Sicherung der Beweise für weitere juristische Aktionen.

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

Grundfragen zur Computer Forensik

Es muss sichergestellt werden, dass soviel Informationen wie möglich von einem kompromittierten System gesammelt werden können, ohne dabei den aktuellen Zustand bzw. Status dieses Systems zu verändern.

> Wie wird der Angriff verifiziert?

> Wie sollte der kompromittierte Rechner und die zugehörige Umgebung gesichert werden?

> Welche Methoden können für die Sammlung von Beweisen verwendet werden?

> Wo sucht man nach Anhaltspunkten und wie können Sie gefunden werden?

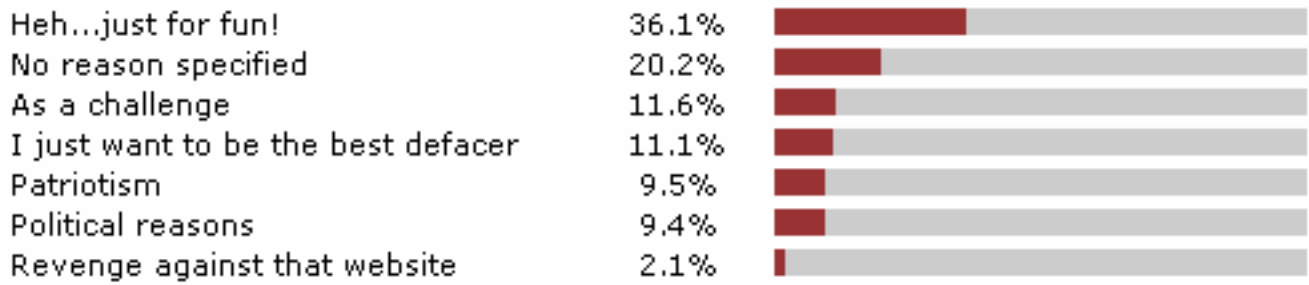
> Wie kann das Unbekannte analysiert werden?

Wer sind die Angreifer?

Hacker (Cracker) mit

- > Sozialer Motivation
- > Technischer Motivation
- > Politischer Motivation
- > Finanzieller Motivation
- > Staatlich-politischer Motivation

By attack reason:



Defacement-Mirror unter http://www.zone-h.org

Fallbeispiel: Motivlage bei Account Missbrauch

> Breit angelegte Ermittlung im Fall von Account Missbrauch am PP Münster

> Erkenntnis über die Tätergruppen:

- Die "typischen Täter" waren männlichen Geschlechts, zwischen 16 und 21 Jahre alt und leben bei den Eltern.
- hatten mittlere bis hohe Computerkenntnisse und
- betrieben den Account-Missbrauch, um sich zu bereichern oder nur auszuprobieren, ob es geht.

Motive	*Fälle*	*in %*
Wirtschaftliche Gründe	307	51,3
Ausprobieren	198	33,1
Technische Möglichkeiten	72	12
Sonstige Gründe	49	8,2
Reinlegen	16	2,7
Gruppen-Anerkennung	9	1,5
Wettkampf	6	1
Anerkennung im Internet	4	0,7
Geheimdienst	2	0,3
Ausspionieren	nicht genannt.	0
Jemanden Schaden zufügen	nicht genannt	0

http://www.bka.de/informationen/account_missbrauch.pdf

Der Innentäter

Der Gesamtverband der deutschen Versicherungswirtschaft (GdV)

> etwa 40 Prozent der ***Betrugs-, Diebstahls- und Unterschlagungsdelikte*** werden von den Mitarbeitern der betroffenen Unternehmen begangen werden

> Im Jahr 2002 Schäden in Höhe von rund 3 Milliarden Euro durch kriminelle Handlungen wie Korruption und Vorteilsnahme, Untreue, Unterschlagung, Diebstahl, Betrug, Wirtschafts- und Betriebsspionage, Verrat von Betriebsgeheimnissen, Erpressung und Insider-Geschäfte.

> höchstwahrscheinlich ist, dass für eine Vielzahl dieser Delikte Computersysteme unterstützend oder begünstigend beteiligt waren.

> Laut Aussage des GdV besitzen die Täter meist betriebswirtschaftliches Fachwissen sowie *gute Kenntnisse der internen organisatorischen Abläufe und Gewohnheiten* des geschädigten Unternehmens.

Der Innentäter

Euler Hermes Kreditversicherungs-AG (Untersuchung von 9000 versicherte Vertrauensschäden → nicht nur Computerkriminalität!)

> Etwa zwei Drittel der Täter waren männlich, ein Drittel weiblich.

> Mit zunehmendem Alter sinkt die Schadenshäufigkeit: 35% der Schäden wurden von Mitarbeitern unter 30 Jahren verursacht. 30% waren zwischen 30 und 40 Jahren alt, 23% zwischen 40 und 50 Jahren. Nur etwa 12% der Schäden gehen auf Mitarbeiter über 50 Jahre zurück.

> Je länger die Betriebszugehörigkeit, desto seltener die Veruntreuung: Die höchste Dichte von Veruntreuungen liegt in den ersten zwei Jahren der Betriebszugehörigkeit, während sie ab 20jähriger Beschäftigung im gleichen Unternehmen minimal ist.

> Es war weiterhin zu erkennen, dass gerade die von langjährigen Mitarbeitern verursachten Schäden oft sehr hoch sind.

Welche Daten können gesammelt werden?

Unabhängig von der konkreten Fragestellung und dem zu untersuchenden System (Server, Workstation, PDA, Router, Notebook etc.) lassen sich grundsätzlich einige empfindliche Datentypen, die für die Ermittlung von Interesse sind, finden:

> Flüchtige Daten

- Informationen, die beim geordneten Shutdown oder Ausschalten verloren gehen (Inhalt von Cache und Hauptspeicher, Status der Netzverbindungen, laufende Prozesse, angemeldete User etc.)

> Fragile Daten

- Informationen, die zwar auf der Festplatte gespeichert sind, aber deren Zustand sich beim Zugriff ändern kann

> Temporär zugängliche Daten

- Informationen, die sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z.B. während der Laufzeit einer Anwendung.

Die Kenntnis um die Halbwertzeit dieser Daten ist sehr wichtig, da damit die Reihenfolge der Datensammlung bestimmt wird.

Fragestellungen für die Ermittlung

- Wer hatte unberechtigten Zugang?
- Was hat der Angreifer auf dem System gemacht?
- Zu welchem Zeitpunkt fand der Vorfall statt?
- Welche Systeme sind zusätzlich betroffen?
- Warum ist gerade dieses Netz oder System angegriffen worden?
- Wie konnte der Angreifer Zugriff erlangen?
- Ist der Angriff vor kurzem geschehen? Was macht der Angreifer jetzt?
- Was konnte der Angreifer auf diesem/von diesem System einsehen?
- Hat der Angreifer etwas zurückgelassen?

Fragestellungen für die Ermittlung

- **Welche Tools kamen beim Angriff zum Einsatz?**
- **Wie kamen diese Tools zum Einsatz?**
- **In welcher Programmiersprache wurden die Tools geschrieben?**
- **Haben diese Dateien Ähnlichkeiten mit Dateien, die auf dem System eines Tatverdächtigen gefunden wurden?**
- **Welche Ereignisse wurden protokolliert ?**
- **Was wird durch die Protokolldaten enthüllt?**
  - > Protokolldaten von Firewall, IDS, RAS, Zutrittskontrollsystemen
- **Was ist auf den Datenträgern gespeichert?**
  - > Welche Spuren sind durch die verwendeten Applikationen hinterlassen worden?
  - > Welche Dateien wurden gelöscht?
  - > Existieren versteckte Dateien?
- **Existieren verschlüsselte Dateien oder -bereiche?**
- **Existieren versteckte Partitionen?**
- **Existieren bekannte Hintertür- oder andere Fernzugriffstools?**

Incident Response als Basis guter Ermittlung

Ziele der Incident Response:

> Bestätigung, dass ein Vorfall stattgefunden hat oder NICHT stattgefunden hat

> Sammeln und Berichten der richtigen und relevanten Informationen

> Etablierung von guten Beweissicherungsmaßnahmen

> Minimierung der Geschäfts- oder Produktionsunterbrechung

> Ermöglichung der strafrechtlichen Verfolgung der Täter

> Erstellen von Handlungsempfehlungen für die Zukunft

Ermittlungsstrategie

Faktoren, die strategiebestimmend sind:

> Wie kritisch sind die betroffenen Systeme?

> Wichtigkeit der gestohlenen oder beschädigten Daten.

> Wer sind die vermutlichen Täter?

> Ist der Vorfall bereits an die Öffentlichkeit gelangt?

> Wie weit ist der Täter bereits gekommen?

> Welche Skills werden beim Täter vermutet?

> Welche Downtime ist zu verkraften?

> Vermuteter finanzieller Gesamtverlust.

Vorgehen sollte durch das Management bestätigt werden.

Eine Technik: Forensische Duplikation

Untersuchung am Live System = Notaufnahme

Untersuchung einer Forensischen Kopie = Pathologie

→Wo ist es wohl stressiger und was gründlicher?

Varianten:

> Entfernen der verdächtigen Festplatte aus dem gehackten System und Anschluss an das Analysesystem

> Anschluss einer zusätzlichen Festplatte an das gehackte System

> Transport der kopierten Daten über ein geschütztes Netz zum Analysesystem

Entscheidung für eine forensische Duplikation

> Kann es zur straf- oder zivilrechtlichen Ahndung kommen?

> Ist es ein breit angelegter und Aufsehen erregender Vorfall?

> Entsteht durch Produktionsausfall ein hoher Verlust?

> Entsteht durch Zerstörung ein hoher Verlust?

> Müssen Daten als Beweis wieder hergestellt werden?

> Muss der freie Speicherbereich durchsucht werden?

Wonach wird auf dem System gesucht?

> Timestamps des Systems

> Trojanisierte Systemprogramme

> Versteckte Dateien und Verzeichnisse

> abnorme Dateien oder Sockets

> abnorme Prozesse

> Häufig genügt ein einziger Ansatzpunkt!

Weitere Fragestellungen

> Kann der Tatverdächtige seinen Standort durch die Verwendung mehrerer Computer verschleiern?

> Kann ein geschriebener Angriffscode oder ein verräterisches Dokument oder eine E-Mail in Verbindung zum Tatverdächtigen gebracht werden (z.B. durch Stil, Vokabular, bestimmte Redewendungen oder enthaltene Datenspuren)?

> Können die gefundenen Spuren über besuchte Webseiten oder heruntergeladene Dateien mit dem Sachverhalt in Verbindung gebracht werden?

> Finden sich Hinweise auf E-Mails oder Chat-Rooms bzw. IRC-Channels, die eventuelle Mittäter oder -wisser identifizieren könnten?

Weitere Fragestellungen

- War für die Durchführen der strafbaren Handlung physischer Zugang zum System nötig?
- Welche Personen hatten außer dem Tatverdächtigen noch Zugang zu dem Computer?
- War auf dem PC ein Cronjob oder Scheduler aktiv, der die verdächtige Handlung ohne Anwesenheit des Tatverdächtigen durchführen konnte?
- Existieren weitere Beweise, die die Aussagen der digitalen Spuren bestätigen oder diesen möglicherweise wiedersprechen?
- Über welche Computerkenntnisse verfügt der Tatverdächtige bzw. dessen Mittäter wirklich, und welche Kenntnisse und Hilfsmittel waren für die Tatdurchführung nötig?

Häufige Fehler bei der Ermittlung

> Keine durchgängige Dokumentation der durchgeführten Aktionen
  - Jeder Vorgang am oder mit dem Beweis muss lückenlos dokumentiert sein

> Entscheidungsträger sind nicht oder nur unzureichend informiert

> Digitale Beweise sind unzureichend vor Veränderung geschützt

> Keine rechtzeitige Meldung über den Vorfall

> Unterschätzen der Tragweite des Vorfalls

> Keinen Incident Response Plan in Vorbereitung

Dinge, die vermieden werden sollten

> Verändern von Zeitstempeln auf den gehackten Systemen (MAC-Times)

> Beenden eines verdächtigen Prozesses auf dem System

> Security Patch installieren, bevor das Response Team weitere Maßnahmen empfiehlt

> Kommandos ausführen, die niemand protokolliert hat

> Tools mit grafischen Interface lokal verwenden

> Nicht vertrauenswürdige Programme und Systemtools verwenden

> Zerstören von möglichen Beweisen durch Installieren oder Deinstallieren von Software

> Zerstören von möglichen Beweisen durch Programme, die Output auf der Beweisplatte generieren

> unter Umständen auch Shutdown

Fragen?!

Kontakt

Anschrift

HiSolutions AG
Bouchéstraße 12
D-12435 Berlin

Fon: +49 30 533289-0
Fax: +49 30 533289-99
www.hisolutions.com

Information Security

Alexander Geschonneck
Leitender Sicherheitsberater
geschonneck@hisolutions.com

http://computer-forensik.org