


IT - Security Forum #5

PROFESSIONAL COMPUTING
netzwoche



Netzwerk Forensik

Ronny Fischer
Security Consultant
CA Schweiz
Ronny.Fischer@ca.com



IT - Security Forum #5

PROFESSIONAL COMPUTING
netzwoche



Agenda

- Was und Wo
 - Was ist Forensik und
 - Wo wird sie eingesetzt ?
- Wie
 - Wird bei einer forensischen Analyse vorgegangen ?
- Ein leistungsfähiges Werkzeug für die Netzwerk Forensik.
 - CA
eTrust™ Network Forensics

95

Was und Wo?

*Was ist Forensik und
wo wird sie eingesetzt ?*

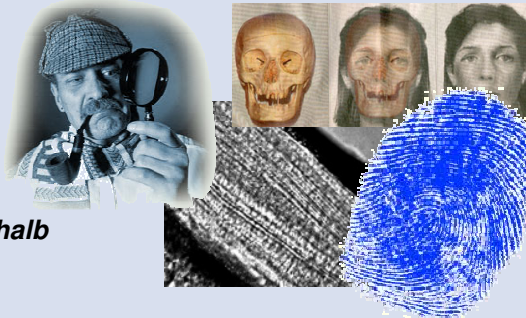
96

WAS bedeutet Forensik ?

Der Begriff der **Forensik** stammt vom lat. forum = **der Marktplatz, das Forum**, da vormalig **Gerichtsverfahren, Untersuchungen, Urteilsverkündungen** sowie der **Strafvollzug** öffentlich und meist auf dem Marktplatz durchgeführt wurden. Daher bezeichnet das Attribut forensisch alles, was gerichtlichen oder kriminologischen Charakter hat.

In der kriminologischen Forensik geht es primär darum, Beweise zu finden, die vor Gericht standhalten. Vereinfacht gesagt versucht die Kriminal Forensik **Beweise für folgende Fragen zu liefern** :

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



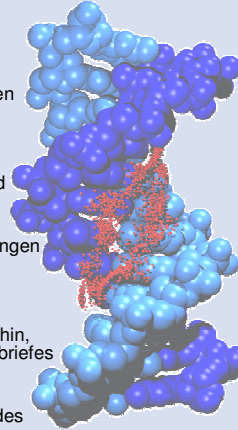
97



Moderne Kriminal Forensik

Die Spezialgebiete der Kriminal Forensik sind vielfältig.
Hier einige Beispiele aus der modernen Kriminal Forensik :

- **forensische Traumatologie** im Sinne der Rechtsmedizin
 - befasst sich mit körperlichen Verletzungen,
- **forensische Entomologie**,
 - befasst sich mit der Aufklärung der Todesumstände mittels der Interpretation von Insektenfunden bei Leichen
- **forensische Toxikologie**
 - befasst sich mit dem Nachweis von Giften
- **forensische Serologie**
 - beschäftigt sich mit der Auswertung von Blutspuren und anderen Sekreten
- **forensische Ballistik**
 - vergleicht und beurteilt Geschosse und Geschosswirkungen
- **forensische Daktyloskopie**
 - wertet Fingerabdrücke aus
- **forensische Linguistik**
 - untersucht Sprache auf einen kriminologischen Aspekt hin, z.B. bei der Feststellung des Urhebers eines Erpresserbriefes
- **forensische Osteologie**
 - identifiziert Personen anhand des Skeletts, die forensische Odontologie versucht das gleiche anhand des Gebisses.



98



IT Forensik

Die IT Forensik unterscheidet primär zwei forensische Spezialgebiete :

Die Computer Forensik

Hierbei geht es darum mittels spezieller **Analyse** von **Datenträgern** einen bestimmten Beweis zu erbringen. Da diese Beweise in der Regel auch einem Gericht vorgelegt werden, ist es elementar, dass die Daten während der Analyse auf keinen Fall verändert werden. Wird nur ein einziges Byte verändert, ist der Beweis vor Gericht nicht mehr aussagekräftig.

Die Netzwerk Forensik

Hier werden in der Regel **Beweise innerhalb** eines **Kommunikationsverhaltens** gesucht. Sind die Beweise in Form eines "Network-Captures" vorhanden, können diese Daten mit geeigneten Werkzeugen in Echtzeit wiedergegeben werden.



99

Computer Forensik, Definition

Die Computer Forensik ist als Anwendung der Informatik auf jede Art von gespeicherten Daten zum Zweck der **Spurensuche** und **Beweissicherung** zu betrachten. Damit die Ergebnisse gerichtlich als Beweise verwertbar sind, gilt es gewisse Prinzipien zu beachten.

Dazu zählen vor allem:

- **Datenverluste minimieren**
- **Alles aufzeichnen, möglichst nichts verändern**
- **Analysen nur auf Kopien durchführen (never touch original)**
- **Ergebnisse neutral, überprüf- und nachvollziehbar präsentieren.**

Daraus kann man den folgenden Prozess einer forensischen Untersuchung ableiten:

- **Erstellen** eines forensisch korrekten **Abbilds** der elektronisch gespeicherten Daten (forensic sound imaging)
- **Authentifizierung** dieses Abbilds
- **Analyse** der gespeicherten Daten
- neutrale, sachlich fundierte und unparteiische **Berichterstattung** in Form eines Gutachtens.

100

Netzwerk Forensik, Definition

In der Netzwerkforensik gelten prinzipiell die gleichen Grundsätze wie in der Computer Forensik. Zusätzlich unterscheiden wir aber zwei Hauptbereiche :

- **Datensammlung**
 - Netzwerkverkehr muss auch in sehr schnellen Netzwerken (GB und mehr) ohne Verlust von Paketen in Echtzeit auf geeignete Datenträger gespeichert werden können.
- **Datenauswertung**
 - Muss grosse Mengen von Daten schnell, einfach, transparent und nachvollziehbar **analysieren**.
 - Netzwerktechnologie ist kompliziert, darum ist es elementar dass die Daten auch für **Laien nachvollziehbar dargestellt werden**.
 - Um Beweise zu erarbeiten die Übertretungen dokumentieren sollten die Kommunikationsprotokolle und Nodes **visuell dargestellt** werden.

101

Gründe für die Netzwerkforensik

Der Gesamtverband der deutschen Versicherungswirtschaft

- etwa **40 Prozent** der Betrugs-, Diebstahls- und Unterschlagungsdelikte werden von den **Mitarbeitern der betroffenen Unternehmen begangen**.
- Im Jahr 2002 **Schäden** in Höhe von rund **3 Milliarden Euro** durch kriminelle Handlungen wie **Korruption** und **Vorteilsnahme, Untreue, Unterschlagung, Diebstahl, Betrug, Wirtschafts- und Betriebsespionage, 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.

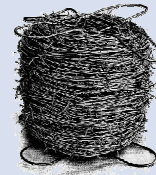


102

DIE Ergänzung zu bestehender IT Security

Wenn wir Netzwerkforensik im **Zusammenspiel** mit weiteren **IT-Sicherheitstechnologien** betrachten und versuchen einen Vergleich mit der richtigen Welt zu ermöglichen würde das folgendermassen aussehen :

- Die **Firewall** ist der **Zaun** der unser Grundstück vor ungebeten Gästen schützt.
- Sollte doch einmal jemand durch den Zaun auf unser Grundstück gelangen, wird das **IDS/IPS**, also die **Alarmanlage** uns darüber informieren.
- Sollte es uns entgangen sein, dass uns die Alarmanlage informiert hat, können wir mit Hilfe der **Videoüberwachung**, also der **Netzwerkforensik** jederzeit beweisen wer, wann, was, wie auf unserem Grundstück gemacht hat.



103

GO OUT
IT-SECURITY
HOSTING

klubschule
MIGROS

Microsoft

visana
Wir tragen Sorge.

ca

IT - Security Forum #5

PROFESSIONAL
COMPUTING

netzwoche

104

Wie ?

wird bei einer forensischen Analyse vorgegangen ?

GO OUT
IT-SECURITY
HOSTING

klubschule
MIGROS

Microsoft

visana
Wir tragen Sorge.

ca

IT - Security Forum #5

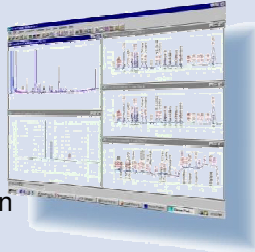
PROFESSIONAL
COMPUTING

netzwoche

105

Grundregeln in der IT-Forensik

- IT-Forensik wird in der Regel durchgeführt, **nachdem** etwas vorgefallen ist (reaktiv).
- Forensisches Arbeiten erfordert die **Dokumentation** jedes ausgeführten Schrittes.
- Die klassischen Maßnahmen des "**Incident Response**" - das System so schnell wie möglich wieder zum Laufen zu bringen - steht in direkter Konkurrenz zu den Maßnahmen der IT-Forensik.
- Die zu sichernden **Daten** müssen (sofern möglich) während des Sicherungsvorgangs und allen weiteren Prozessen **unverändert** bleiben.
- Die **Integrität** der Daten muss zu jedem Zeitpunkt gesichert sein.



Fragen vor der forensischen Analyse

Bevor mit der Analyse der Daten begonnen wird, sollten folgende Fragen gestellt werden :

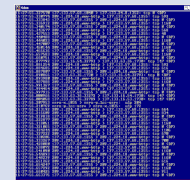
- Gibt es einen Notfallplan — ist dieser überhaupt anwendbar?
- Welche konkreten Aufgaben haben Priorität (Spurensicherung, Wiederanlauf der Systeme, Absicherung der Systeme)
- Sollen Polizei und Staatsanwaltschaft eingeschaltet werden?
- Soll das System vom Netz genommen werden?
- An welcher Stelle erfolgte der Zugriff?
- Wie erhielt der Angreifer Zugriff?
- Von welcher Stelle ging der Angriff aus?
- Was war das Ziel des Angreifers?
- Wer ist der Angreifer?
- Welcher materielle Schaden ist entstanden?
- Welche Daten wurden modifiziert, gelöscht oder hinzugefügt?
- Welche Änderungen am System wurden vorgenommen?



106

Datensammlung (Netzdaten)

- Eine Empfehlung der Fachgruppe Security der Schweizer Informatiker-Gesellschaft (fgsec) in der Broschüre Forensic Computing unter **Ausgewählte präventive Informatik-Massnahmen gegen Hacking / Spionage** lautet unter anderem : **"permanente real-time Überwachung der Netzwerke und Zugriffsschutzsysteme"**.
 - http://www.adverum.ch/download/Forensic_Computing.pdf
- Dies scheint in der Netzwerk Forensik der wirklich einzig gangbare Weg zu sein, da nur **durch lückenlose Aufzeichnungen sichergestellt** wird, dass die **kompletten Kommunikationsbeziehungen aufgezeichnet** wurden.
- Geräte und Techniken mit denen Netzwerkdaten ohne Verlust auf Datenträger gespeichert werden können sind im Internet genügend vorhanden. Dieses Problem sollte mit relativ wenig Aufwand realisierbar sein.
 - Tcpdump
 - <http://www.tcpdump.org>
 - Ethereal
 - <http://www.ethereal.com>
 - Sniffer
 - <http://www.sniffer.com>



107

Datenauswertung (Netzdaten)

Die **Auswertung** der Daten ist definitiv die **grösste Herausforderung** in der Netzwerkforensik.

Wenn man viele GigaByte von Netzwerkdaten zu analysieren hat und meistens nicht einmal weiss nach was genau man suchen muss, sind professionelle Werkzeuge zur Analyse unumgänglich.

Ein flexibles und leistungsfähiges Werkzeug zur Auswertung von Netzwerkdaten und Log-Dateien aller

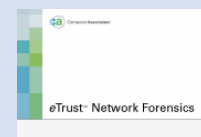
Art ist **eTrust™ Network Forensics** der Firma Computer Associates.



108

Historie von eTrust™ Network Forensics

- **1999** lizenzierte das **NSA's** Office of Research and Technology Application in Zusammenarbeit mit dem US General Counsel for Technology Software Code an die Rüstungsfirma **Raytheon**.
- Als direktes Resultat aus diesem Technologie-Transfer entwickelte **Raytheon** aus diesem Software Code ein Produkt mit dem Namen **Silent Runner**.
- **Silent Runner** wurde darauf an Abteilungen des **Departements of Defense**, an die NSA und kommerzielle Anwender in Lizenz verkauft.
- Im **July 2003 verkaufte Raytheon** Silent Runner mit allen Rechten an die Firma **Computer Associates**.
- **Computer Associates** führt die Software nun unter dem Namen **eTrust™ Network Forensics** in der eTrust Security Produktelinie und hat einige Teile des Source Code auch in andere CA Produkte (Unicenter etc.) einfließen lassen.



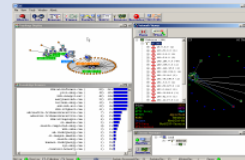
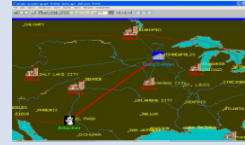
109



Einsatzbereiche von eTrust™ Network Forensics

eTrust™ Network Forensics hilft bei:

- Der **Überwachung** und **Rekonstruktion** von **Kommunikations-Verkehr** im Netzwerk.
- **Überwachung auf Einhaltung von „Regeln“**.
 - Entdeckt Missbrauch von Netzwerkressourcen.
 - Aufspüren von Policy-Verletzungen.
- **Analyse** von **Kommunikationsbeziehungen** bis auf **Anwendungs-Ebene** (Geschäftsprozesse).
- **Schützt geistiges Eigentum** und vertrauliche Informationen.
 - Blinde oder gezielte Kontextanalyse.
- Sammeln von Informationen für das **Risiko-Management**.
 - Visualisiert die Netzwerkbenutzung.
 - Hilft komplexe Prozesse einfacher zu verstehen.
 - Analysiert, korreliert, Daten von verschiedenen Quellen wie IDS/IPS etc.

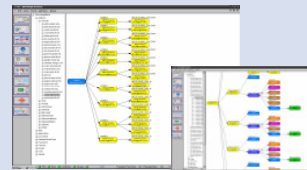
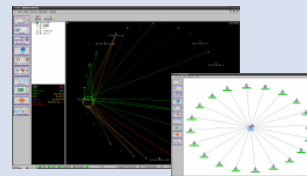
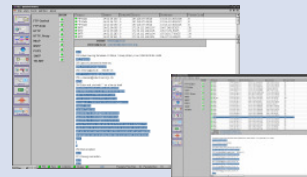


110



eTrust™ Network Forensics Collector

- Klartext Protokolle werden in Echtzeit in verständliche Nachrichten dekodiert.
- Kommunikations-Beziehungen werden übersichtlich in Echtzeit dargestellt.
- Beziehungen zwischen Benutzern, IP Adressen, DNS Namen etc. können einfach eruiert werden.

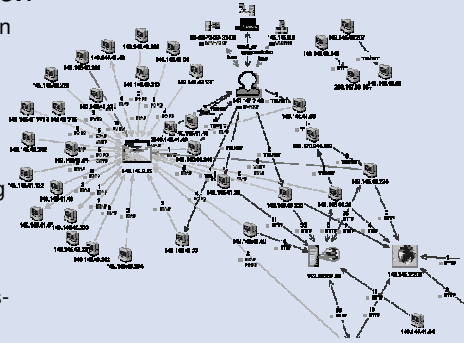


111



eTrust Network Forensics Analyzer

- Der eTrust™ Network Forensics Analyzer bietet eine **2D Darstellung von Node Kommunikationsbeziehungen**.
- Diese Darstellung erlaubt eine einfache Analyse des Verkehrsflusses und **hebt Anomalien** im Verhalten der Protokolle **speziell hervor**.
- Die Nodes und die Beziehungen sind **interaktiv** und können bei einem Mausklick weitere Informationen preisgeben.
- Durch die "**Time sequencing**" Funktion wird die Untersuchung massgeblich erleichtert.
- Durch das originalgetreue Animieren der Kommunikationsdaten werden **Anomalien** (wie z:Bsp. Portscans) **schnell identifiziert**.

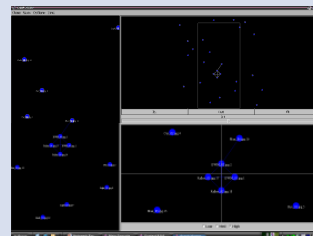
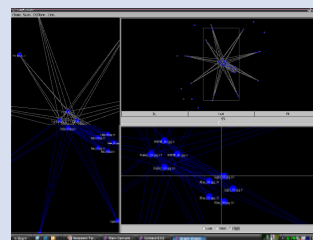


112



Context Management

- Das Modul „**Context Management**“ dient zur optischen Analyse von Daten und analysiert mit n-gramm Technologie nach dem Prinzip der „Ähnlichkeit“.
- Durch den Einsatz von **n-grams** und **Analyse** auf **Bit-Ebene** ist das Context Management Modul Datei-Format-unabhängig.
- **Ähnliche Daten** werden zu „**Clustern**“ gruppiert.
- Die Angleichung der Daten wird über einen „Schieberegler“ realisiert.
- Daten können auch nach bestimmten **Schlüsselwörtern** durchsucht werden.



113



Summary

- *eTrust Network Forensics* ist ein **Netzwerk Discovery-, Analyse- und Visualisierungswerkzeug** das zur Verteidigung des geistigen Firmeneigentums eingesetzt wird.
- *eTrust Network Forensics* identifiziert **Sicherheitsrisikos und Netzwerk Verletzbarkeiten** und alarmiert das Management über den evt. Verlust von Daten.
- *eTrust Network Forensics* ist das einzige Produkt das durch die **Möglichkeit der Korrelation** von komplexen Netzwerk Ereignissen rasche Gegenmassnahmen ermöglicht
- *eTrust Network Forensics* hilft beim:
 - **internen Schutz von geistigem Eigentum**
 - **Missbrauch von Ressourcen**
 - **Netzwerk Risikoanalyse.**
 - **Netzwerk Forensik.**
 - **maximieren des Wert von IDS, FW, etc. Logdaten**

