Janotta und Partner
Cybersecurity

IT Forensik -
Von Digital bis IT, dem Täter auf der Spur.

Objektive Beweise, mit der IT Forensik.

Auf die IT-Forensik, auch Computer Forensik oder digitale Forensik genannt, übertragen, bedeutet dies also die Aufklärung von Vorfallen im digitalen Bereich. Man sucht also nach digitalen Spuren, die genau wie in den anderen Gebieten der Forensik, Hinweise auf einen Tathergang liefern sollen. Nur sind die Spuren in diesem Fall nicht biologischer Art, sondern physischer Art, da die Informationen magnetisch oder optisch auf einer Festplatte oder einem anderen physikalischen Speichermedium gespeichert sind.

Das Ziel: Digitale Spuren suchen und Aufklärung von Cyberkriminalität

In der heutigen Zeit spielt die Optimierung von Verfahren durch Prozessmanagement eine tragende Rolle. **Incident Response** Prozesse werden von jeder Firma selbst definiert, folgen aber generell einem einheitlichen Schema. Jeder Vorfall löst einen Incident Response Prozess aus, auch wenn zunächst nicht feststeht um was für einen Vorfall es sich handelt, z. B. Sicherheitsverletzung oder Normale Betriebsstörung. Erst bei der Datensammlung innerhalb des Prozesses wird sich herausstellen um welche Art von Vorfall es sich handelt und anhand dessen wird entschieden, wie die richtige Response Strategie aussehen muss. Dabei wird schnell klar, dass es unterschiedliche Response Strategien geben muss, denn eine Sicherheits-Verletzung wirft andere Fragen auf als ein Betriebsausfall.

Ein **Incident Response Prozess** soll demnach in erster Linie Handlungssicherheit zur Krisenbewältigung geben und so die Ausfallzeiten gering halten, bzw. eine Grundlage zur weiteren Untersuchung bieten. Genau dort beginnt die Computerforensik. IT-Forensik ist ein Teilgebiet der IT-Sicherheit, die es ermöglicht Schwachstellen zu ermitteln, Straftäter oder kriminelle Handlungen zu verfolgen und somit die Sicherheitsrisiken für Unternehmen zu vermindern. Mit dem Zweck der gerichtsverwertbaren Beweissicherung werden digitale Spuren gesichert, Interpretiert und dokumentiert.

Grundsätzlich unterscheidet man zwei verschiedene Arten der forensischen Analyse. Das live-response Verfahren und die postmortem Analyse. Die post-mortem Analyse kommt. Bei strafrechtlichen Verfolgungen häufiger vor und beschreibt die Analyse eines ausgeschalteten Systems. Hierbei werden die digitalen Spuren auf einem forensischen Duplikat analysiert,

Kennen Sie das Risiko dem Sie ausgesetzt sind?

Hackern den entschiedenen Schritt voraus. Schützen Sie was zu Schützen ist.

AUF DEN EURO KOMMT ES AN. UNTERNEHMEN UND WIRTSCHAFT SIND STÄNDIGEN BEDROHUNGEN AUSGESETZT.

Schützen Sie Ihre Wirtschaftsleistung und Ihre Daten, damit geheimes geheim bleibt und privates privat.

GUTE ZEIT

Ihr Sicherheits-potenzial liegt bei ca 30%

NOCH BESSERE NEUIG KEITEN

Durch optimierte Arbeitsweise Sparen Sie Kosten!

Reverse Engineering und IT Forensik – Wie?

Eine IT-forensische Untersuchung findet immer statt, sobald ein kriminalistischer Vorfall stattgefunden hat oder angenommen wird. Eine Betriebsstörung oder zufälliger Ausfall ohne Außeneinwirkung bedingen also keiner forensischen Untersuchung. Um die Vorfälle zu klassifizieren und eine einheitliche und verständliche Definition des Vorfalls zu gewährleiste, wurde die CERT-Taxonomie 2 eingeführt Diese Taxonomie klassifiziert den Vorfall in drei Bereiche, die ineinander greifen: Vorfall, Angriff und Ereignis.

d. h. auf einem bitweise kopierten des kompromittierten Systems. Die postmortem Analyse hat den Vorteil, dass beliebig viele Kopien der Datenträger erstellt werden können ohne Beweise zu vernichten oder zu verändern.

Damit können unterschiedliche Analyseverfahren gleichzeitig durchgeführt werden und sind zeitlich unbegrenzt. Nachteile der post-mortem Analyse sind allerdings, dass kaum Aussagen über diese Laufzeit des Systems gemacht werden können und flüchtige Daten meist durch das Ausschalten des Systems verloren gehen und damit nicht analysiert werden können. Im Gegensatz zum live-response Verfahren kann das Originalsystem schon wieder dem Betrieb zur Verfügung gestellt werden, ohne dass die Untersuchungen abgeschlossen sein müssen.

Live-response Analysen der Forensik“

Live-response Analysen lassen hingegen auch eine Analyse von flüchtigen, fragen temporär angeglichenen Daten zu. Diese Daten stehen im abgeschalteten System nicht zur Verfügung, weil sie Informationen über Prozesse, Verbindungen oder den Inhalt von Caches enthalten und nach einem herunterfahren des Systems gelöscht oder verändert werden. Diese Daten bilden auch den Schwerpunkt von live-resonse Analysen.

Die beiden grundsätzlichen Arten der Analyse werden jedoch oft auch in Kombination angewandt, so dass ein optimales Ergebnis erzielt werden kann ohne dass ein System lange Zeit nicht zur Verfügung steht.

Jede forensische Ermittlung baut auf dem Prinzip des Spur-Annahme-Beweis Kreislauf auf. Ziel einer forensischen Untersuchung ist also Beweise zu erbringen, die eine Annahme belegen das ein System kompromittiert wurde. Dazu soll eine forensische Untersuchung belegen, wann das System gehackt wurde, wer als möglicher Täter in Frage kommt und welche Sicherheitslücke ausgenutzt werden konnte um in das System einzudringen. Weiterhin soll die forensische Analyse die Ausmaße des Schadens feststellen und die Beweise des Vorfalls juristisch verwertbar sichern.

Prozess und Methoden der IT Forensik

Das verbreitetste Modell einer IT-forensischen Analyse ist das SAP. Der Name setzt sich bereits aus den drei Phasen des Modells zusammen: Secure, Analyse und Present. Man kann die drei Phasen in Beweissicherung, Analyse der Daten und abschließend die sogenannte Präsentation. In der ersten, der so genannten Secure Phase, werden alle Daten sorgfältig erfasst. Dies wird unter anderem dadurch sichergestellt, dass die Datensammlung von Expertenteams durchgeführt wird, die nach dem Vier-Augen-Prinzip arbeiten. Zusätzlich sollten auch Maßnahmen ergriffen werden, die es einem möglichen Innentäter erschweren nachträglich seine Spuren zu verwischen. Beweissicherung spielt in der Secure Phase die zentrale Rolle. Wenn zu Beginn der Ermittlungen noch nicht feststeht ob eine Verfolgung des Vorfalls überhaupt vorgenommen wird, sollten alle Beweise so gesichert, protokolliert und dokumentiert werden, dass die juristische Glaubwürdigkeit erhalten bleibt.

In der zweiten Phase, der Analyse-Phase, werden gesicherte Spuren und Beweise sorgfältig und objektiv bewertet. Auch technischen Laien muss der Ermittlungsprozess nachvollziehbar durch uns dargelegt werden.

Weshalb Janotta & Partner?

- Informationssicherheit ist unser Geschäft: Profitieren Sie von unserem erfahrenen Expertenteam!
- Auf die Prozesse kommt es an: Lassen Sie uns zunächst Ihre bestehenden Abläufe analysieren und optimieren.
- Am effektivsten – Komplettlösung: Wir stehen für die umfassende Gesamtlösung, von der Beratung über die vollständige Integration in Ihre IT Umgebung bis hin zur kontinuierlichen Optimierung Ihrer Sicherheit.
- Ihr Schlüssel zum Erfolg – der richtige Partner: Eine unschlagbare Kombination: unsere umfassende praktische Erfahrung gepaart mit der Zuverlässigkeit und dem Knowhow eines Experten Teams.

Janotta und Partner
Cybersecurity

Recovering Traces: Die Digitale IT-Forensik

- Zur IT Forensik zählt auch Reverse Engineering.
- Zur IT Forensik zählt auch Forensik auf Android.
- Netzforensik ist ein Teilgebiet der Digitalen Forensik.
- IT Forensik sichert Beweise und kann Täter überführen.
- IT Forensik kann dabei helfen, Spuren zu sichern und Überwachung zu enttarnen.
- IT Forensik hilft Unternehmen nach Hacker Attacken.
- Durch die IT Forensik ist es möglich Malware und Trojaner zu analysieren.
- IT Forensik ist objektiv.

Janotta und Partner: Ihr Ansprechpartner

Janotta und Partner
Cybersicherheit
Breslaustrasse 28
97424 Schweinfurt
Tel.: +49 (09721) 370 38 17
Email: info@janotta-partner.de
www.janotta-partner.de

10/2015