TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "IT-Forensik"

Berlin, 12.05.2016

IT – Forensik

"Finden Sie die Nadel im Heuhaufen - Netzwerkanalyse und Forensik zur Beweissicherung und Datenanalyse"

Timur Özcan, NEOX NETWORKS GmbH

Wussten Sie schon?

Durch Internetkriminalität entsteht allein in Deutschland ein wirtschaftlicher Schaden von ca. 58 Milliarden Dollar / Weltweit sogar 400 Milliarden Dollar schaden Quelle: **Net Losses – Estimating the Global Cost of Cybercrime**

Die globale Internetwirtschaft generiert Umsätze von ca. 2 bis 3 Billionen US - Dollar

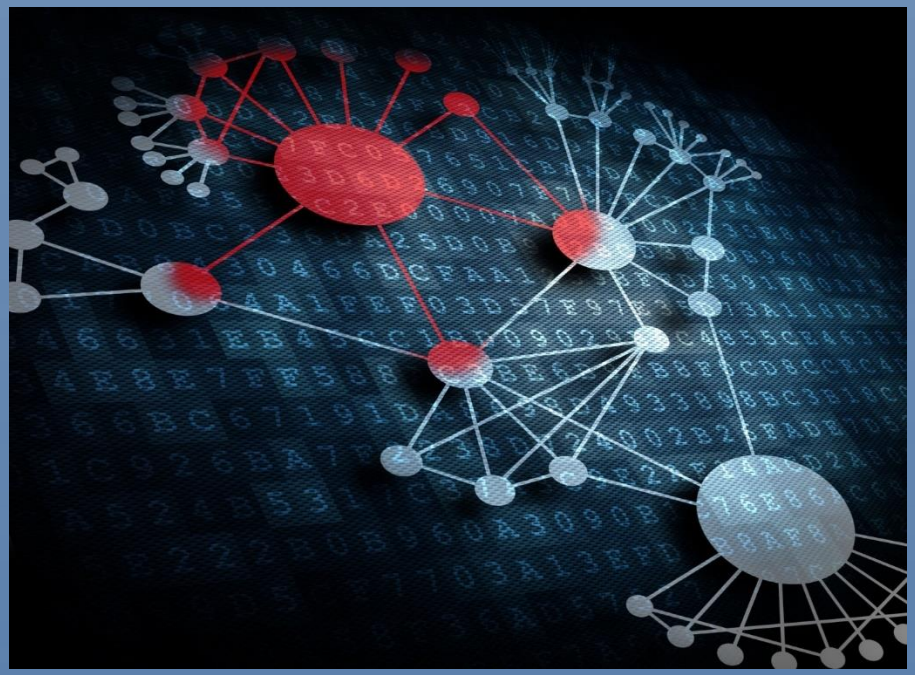
50.000 Webseiten werden pro Tag gehackt

Alle 3 Minuten findet ein Cyber-Angriff auf deutsche Unternehmen statt

Firmen wie Sony und Adobe sowie der deutsche Bundestag waren von zahlreichen Hackerangriffen betroffen und haben einen erheblichen wirtschaftlichen Schaden erlitten

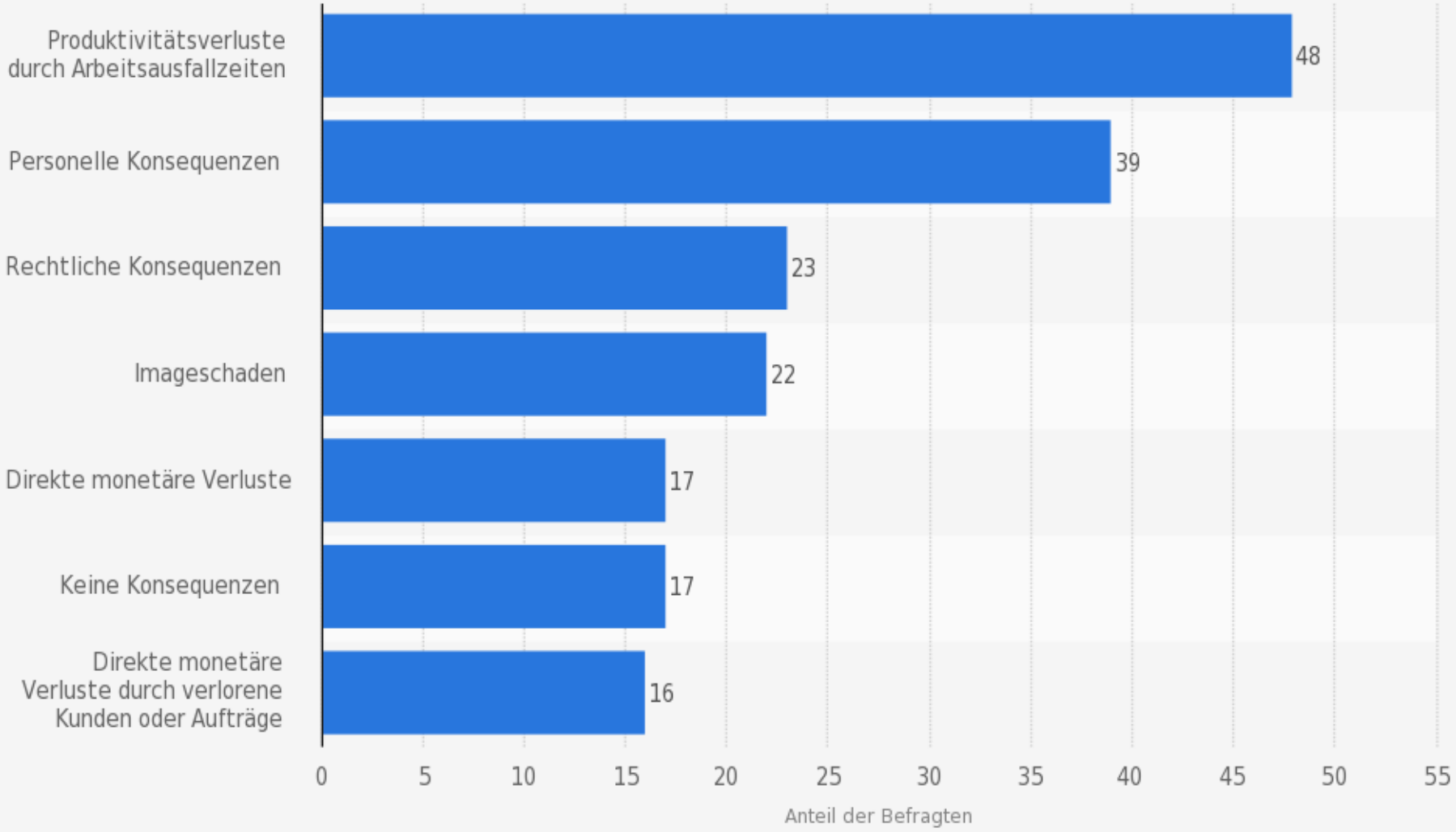
Viele Firmen erkennen die Hackerangriffe nicht oder erst sehr spät (nach 6 Monaten)

Das Netzwerk ist das Nervensystem Ihrer IT…



… und verbindet Daten, Menschen und Maschinen

Welche Folgen ergaben sich aus Angriffen auf die IT-Sicherheit in ihrem Unternehmen?

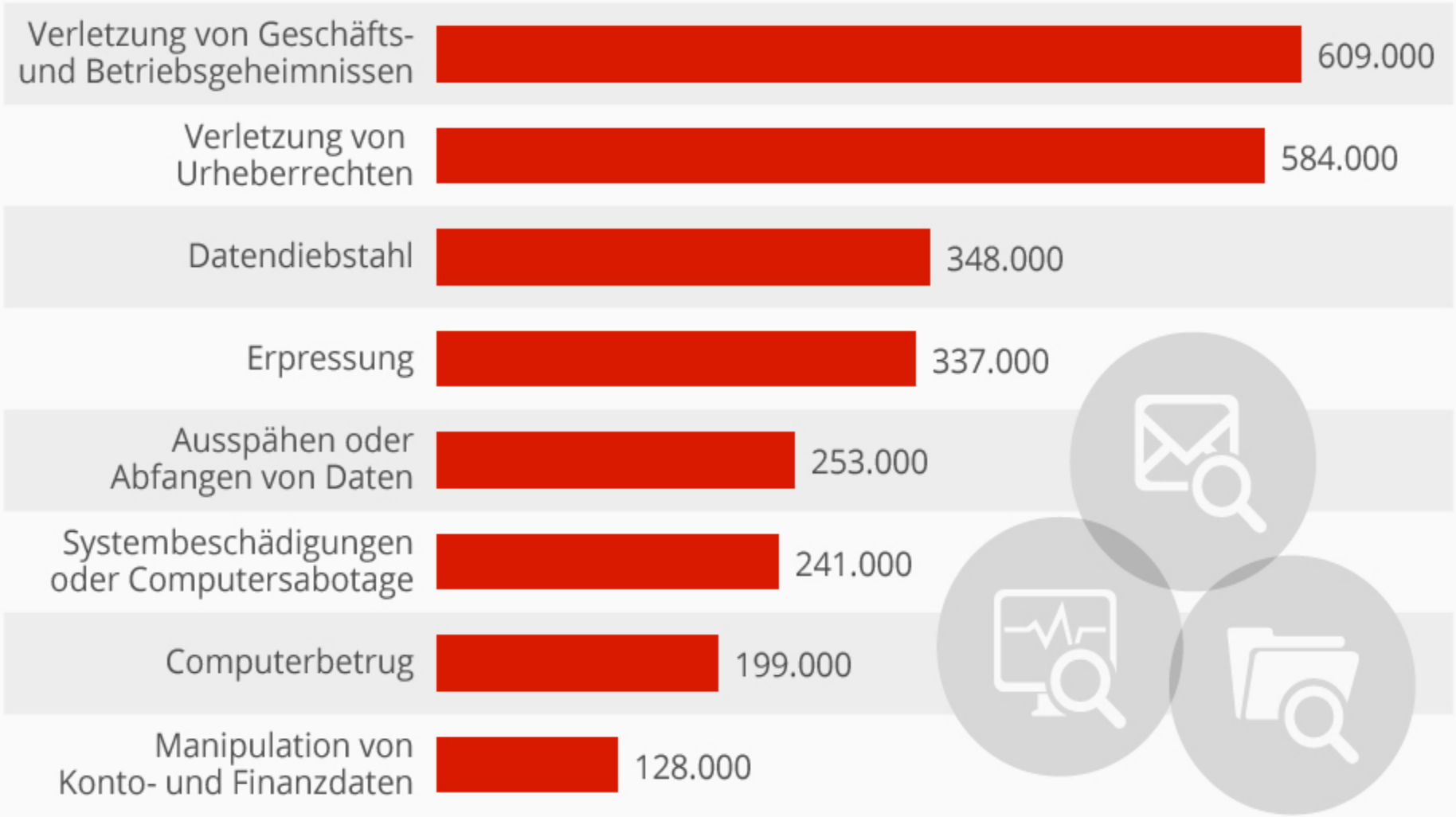


Source::
IDC

Weitere Informationen:
Deutschland; 2010; 146 Respondents; Deutsche Unternehmen mit mehr als 100 Mitarbeitern

Cybercrime kommt Unternehmen teuer zu stehen

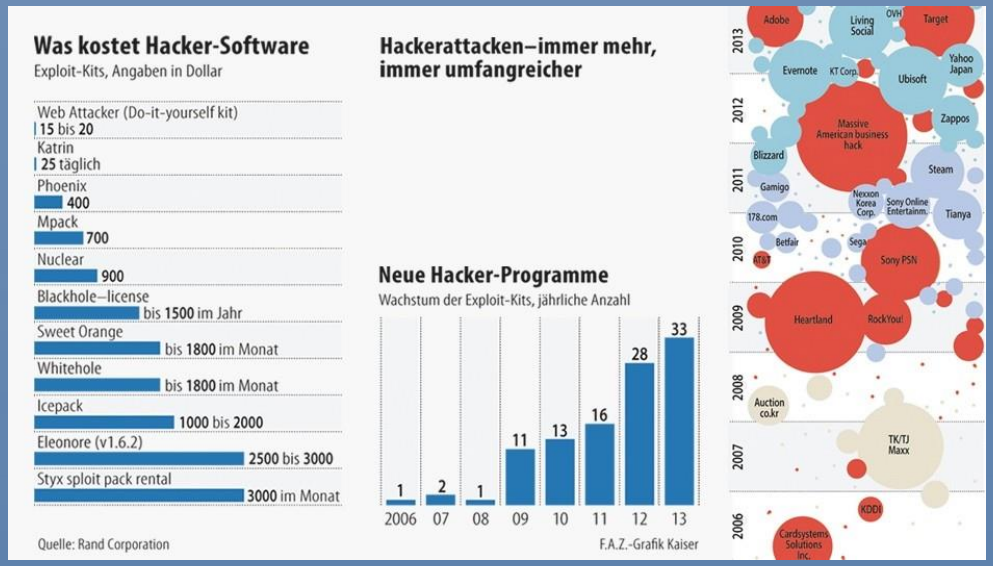
Durchschnittliche Schadenshöhe pro E-Crime-Fall bei Unternehmen in Deutschland (in Euro)



Basis: 505 repräsentativ nach Branche und Umsatz ausgewählte Unternehmen

Quelle: KPMG | e-Crime 2015

Hacking, eine Industrie für sich!



Mittlerweiler profitabler als der Drogenhandel!

http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/computerkriminalitaet-profitabler-als-drogenhandel-12871348.html

Studie: Hackerangriffe werden zu spät entdeckt

- ca. 229 Tage brauchen Unternehmen, um eine Kompromittierung zu erkennen
- lange Reaktionszeit macht den Hackerangriff und dessen Folgen immer kostspieliger
- Im Schnitt entstehen 3,8 Millionen Dollar Schaden pro Unternehmen (2014) / das macht ein Anstieg von 23% zum vorherigen Jahr (2013)
- Für die Studie wurden 350 Unternehmen befragt aus elf Ländern, darunter auch Deutschland mit dem Durchschnitt von 3,5 Millionen Dollar Schaden pro Unternehmen
- Angriffe führen vermehrt zu Kundenfluchtaktionen -> sinkende Umsätze -> macht sich in jeder Hinsicht bemerkbar
- 211 Dollar Schaden pro Datensatz, knapp hinter U.S.A mit 217 Dollar Schaden pro Datensatz
- Verlorenes Vertrauen wird immer teurer

Quelle: http://deutsche-wirtschafts-nachrichten.de / „2015 Cost of Data Breach Study"

Vorgehensweise eines Angreifers

Ein Angriff setzt sich aus folgenden Phasen zusammen:

Nach den NSA-Skandalen wird das Thema Netzwerksicherheit wieder stärker in der Bevölkerung wahrgenommen. Jedes Unternehmen besitzt in der Regel einige Mechanismen, um sich gegen externe Bedrohungen zu schützen. Allerdings werden die meisten Angriffe nach wie vor aus dem inneren Netzwerk geführt.

Haben Sie dieses Szenario ebenfalls schon in Ihrer Sicherheitsstrategie betrachtet?

Von daher ist es wichtig schon in der Aufklärungsphase einen Angriffsversuch zu erkennen!

Big Data

Giga-, Tera-, Petabytes – die Menge der weltweit erzeugten, gespeicherten und übertragenen Daten ist schwindelerregend. Eine Daten-Datensammlung

VON MELISSA MONTASSER

1 Kilobyte:
1.000 Byte

1 Megabyte:
1.000.000 Byte

1 Gigabyte:
1.000.000.000 Byte

1 Terabyte:
1.000.000.000.000 Byte

1 Petabyte:
1.000.000.000.000.000 Byte

1 Exabyte:
1.000.000.000.000.000.000 Byte

Speicherplatz der *Mondlandefähre* von *Apollo 11* von 1969:
74 Kilobyte

Speicherplatz auf der ersten im Handel erhältlichen *Diskette*:
80 Kilobyte

Kapazität der ersten Festplatte (IBM 305 RAMAC, ca. *1 Tonne schwer*):
5 Megabyte

Speicherplatz auf der ersten *SD-Karte*:
8 Megabyte

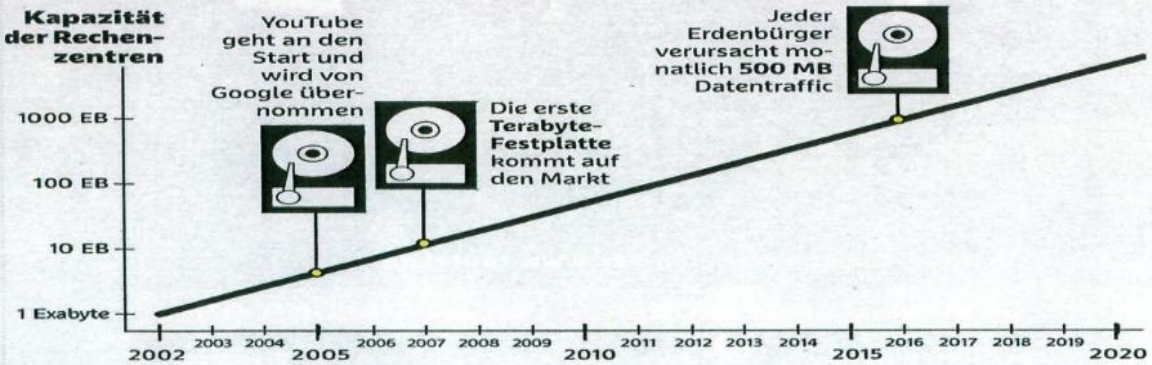
Speicherplatz auf einer heutigen SD-Karte:
***bis zu* 512 Gigabyte**

Durchschnittliche Speicherkapazität einer *externen Festplatte* 2011:
500 Gigabyte

Geschätzte durchschnittliche Speicherkapazität einer externen Festplatte 2020:
3,3 Terabyte

Produzierte Speicherkapazität von Festplatten und SSDs im Jahr 2015:
ca. 700 Exabyte

Datenmenge, die *Google* 2008 täglich verarbeitet hat:
20 Petabyte



Quellen: Seagate, Western Digital, Toshiba, Samsung, IDC, Eigene Interpolation

Datenmenge, die Google 2015 täglich verarbeitet hat:
über 500 Exabyte

Die geschätzte Speicherkapazität aller Rechenzentren *weltweit* 2002:
1 Exabyte

Die geschätzte Speichermenge aller Rechenzentren weltweit 2016:
1.180 Exabyte

Datenmenge einer *Textseite*:
1 Kilobyte

Die *Bibel* als Text:
4 Megabyte

Serverkapazität von *chip.de* (Texte, Videos, Downloads):
ca. 5 Terabyte

Die Gesamtheit aller *gedruckten Werke*
200 Petabyte

Datenbestand in der *Cloud* 2011 (Server plus Endgeräte):
329 Exabyte

Datenbestand in der Cloud 2015:
4.100 Exabyte

Weltweites *IT-Datenvolumen* 2013:
4,4 Exabyte

Geschätztes Datenvolumen 2020:
44 Millionen Exabyte

Datenmenge, die *Steam* wöchentlich an amerikanische Nutzer übermittelt:
16 Petabyte

Datenvolumen, die der Streaminganbieter *Netflix* im vierten Quartal 2014 gestreamt hat:
24 Exabyte

Datenmenge, die das Archiv des *Hubble*-Weltraumteleskops seit 1990 ***gespeichert hat:***
über 100 Terabyte

Datenmenge, die jährlich zu diesem Archiv hinzukommt:
10 Terabyte

Speicherkapazität, um die *YouTube* täglich erweitert werden muss:
1 Petabyte

Erinnerungskapazität des *menschlichen Gehirns:*
2,5 Petabye

Big Data – Data is continuously growing

- 2.7 Zetybytes of data exist in the digital universe today
- According to IBM 2.5 quintillion bytes of data is created every day
- Facebook stores, accesses, and analyzes 30+ Petabytes of user generated data
- Akamai analyzes 75 million events per day to better target advertisements
- 294 billion e-mails sent every day
- 230 million tweets a day
- 5 exabytes of data generated every two days
- 80% of growth in unstructured data
- 35 zetabytes of data generated annualy by 2020!

Herausforderung:
Die wachsende Verwundbarkeit der Netze

Sicherheitsangriffe

- nehmen zu, werden komplexer und immer kostspieliger.

Verlust von Unternehmensdaten

- führt zu wachsenden finanzielle Folgen
- beschädigt das Image
- macht hart erarbeitete Wettbewerbsvorteile zunichte.

Firewalls und andere Schutzvorkehrungen

- sollen Zugriffe auf die unternehmenseigenen Netzstrukturen verhindern
- Trotzdem gelingt es Angreifern, diesen Schutz zu überwinden.

Unterstützung durch Netzwerkforensik

- Im Zusammenspiel mit anderen Sicherheitstechnologien können Sicherheits-Analysten mit den Mitteln der Netzwerkforensik durch lückenlose Aufzeichnung und umfassende Analyse von Netzwerk-Traffic die Beweise für einen Angriff finden.
- In Verbindung mit leistungsstarken Suchfunktionen und Analyse-Tools ermöglicht die Netzwerkforensik Security-Analysten damit das "Finden der Nadel im Heuhaufen", die Identifizierung und die Bestimmung von Angriffsmustern, so dass auf Basis dieser Erkenntnisse Gegenmaßnahmen eingeleitet und die Sicherheitsstrategien entsprechend angepasst werden können.

Netzwerk Forensik? Was ist das eigentlich?

Definition: Netzwerk Forensik

Netzwerkforensik ist das Mitschneiden, Speichern und Analysieren von Ereignissen in einem Netzwerk.

- auch als Packet Mining, Packet-Forensik oder Digitale Forensik bezeichnet

Grundidee

- Jedes einzelne Datenpaket des Netzwerk-Traffics (SMTP, HTTP, ERP, CRM, SQL – sämtlicher Verkehr jeglichen Typs im Netzwerk eines Unternehmens) wird in einem durchsuchbaren Repository aufgezeichnet, damit im Nachgang eine detaillierte Analyse stattfinden kann.

SANS Institut

- „die Netzwerkforensik kann aufdecken, **wer wann, mit wem, wie** und **wie oft** kommuniziert hat. Es kann Adressen in den unteren Schichten miteinander kommunizierender Systeme aufdecken. Analysten können dann Aktivitäten und Konversationen zu einer physischen Applikation zurückverfolgen. Die gesamten Inhalte von E-Mails, IM-Unterhaltungen, Webaktivitäten und Dateiübertragungen können aufgerufen und rekonstruiert werden, um die ursprüngliche Transaktion aufzudecken. Noch wichtiger: Die Protokolldaten aus dem Umfeld der Konversation sind zumeist besonders wertvoll.“

Anforderungen an eine forensische Untersuchung

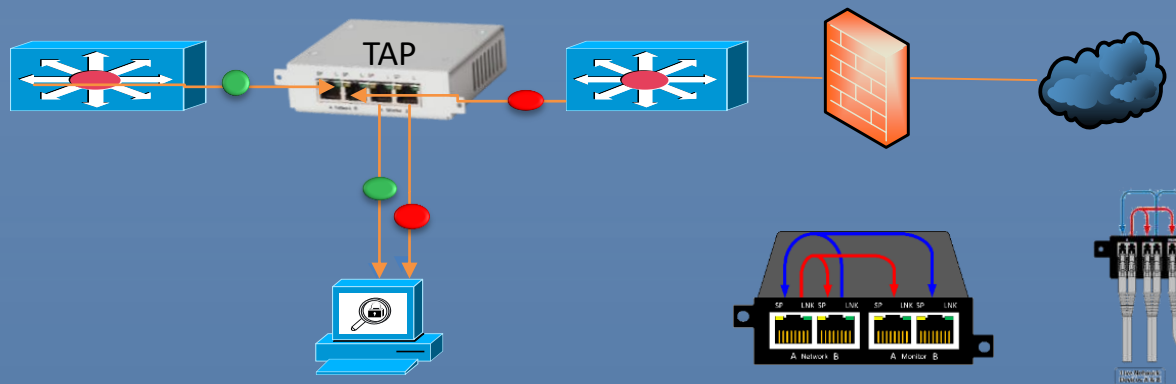
Des Weiteren können die nachfolgenden Fragestellungen relevant werden, insbesondere auch im Fall der Strafverfolgung oder einer Sicherheitsbewertung :

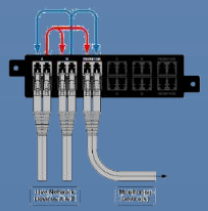
- Wer hat es getan? Wer bewegte bzw. veränderte Daten? Wer war anwesend und beteiligt?
- Was kann gegen eine zukünftige Wiederholung der Vorgänge getan werden?

Dabei muss eine Untersuchung im Sinne der IT-Forensik prinzipiell nach Spuren suchen, welche sowohl eine These untermauern als auch diese widerlegen können.

Passiver Zugriff auf die Netzwerkdaten mittels einem Netzwerk TAP

- Voll-Duplex Abgriff und Analyse ohne Beeinträchtigung der aktiven Netzwerkverbindung
- Layer 1 & 2 Fehler werden mit herauskopiert
- Defekte Pakete oder ungültige Pakete gemäß IEEE 802.3 werden ebenfalls an die Monitoring Ports ausgeleitet
- Datenintegrität sichergestellt, rückwirkungsfrei
- Permanenter Zugriff bei 100% Transparenz
- Unsichtbar im Netzwerk (keine MAC Adresse)
- Taps von 10MBit/s bis 100GBit/s erhältlich (Kupfer, Glasfaser MM, SM)





Netzwerk Forensik - Datenaufzeichnung

- Sicherstellung der originalgetreuen Daten (forensisches Duplikat) und der Beweismittel
- Hash Wert der aufgezeichneten Daten erzeugen und festhalten
- Verschlüsselung der Daten, um einen unerlaubten Zugriff Dritter zu verhindern
- Zeitstempel erzeugen (<1µs) | Externe Zeitquelle (GPS, PTP, etc)
- Einsetzung von „Writeblocker“ auf die gesicherten Daten
- Write to Disk Capturing Verfahren einsetzen, um Paketverluste zu vermeiden
- Spezielle Capture Karten einsetzen, die OS unabhängig arbeiten
- Sicherstellen, dass keine Netzwerkpakete in die aktive Leitung gelangen
- Paket Counter helfen Kapazitätsengpässe zu erkennen
- Hardware Filter in Betracht ziehen

Speicherkapazität für forensische Analysen

	Pro Sekunde	Pro Minute	Pro Stunde	Pro Tag	Pro Woche	Pro Monat	Nach 6 Monaten
1 MBit/s	125 KBytes	7,5 MB	450 MB	10,8 GB	75,6 GB	324 GB	1,944 TB
10 MBit/s	1,25 MB	75 MB	4,5 GB	108 GB	756 GB	3,24 TB	19,44 TB
100 MBit/s	12,5 MB	750 MB	45 GB	1,08 TB	7,56 TB	32,4 TB	194,4 TB
1 GBit/s	125 MB	7,5 GB	450 GB	10,8 TB	75,6 TB	324 TB	1,944 PB
2 GBit/s	250 MB	15 GB	900 GB	20,16 TB	150,12 TB	648 TB	2,888 PB
5 GBit/s	625 MB	3,75 GB	2,25 TB	54 TB	378 TB	1,62 PB	9,77 PB
10 GBit/s	1,25 GB	75 GB	4,5 TB	108 TB	756 TB	3,24 PB	19,44 PB

Netzwerk Forensik - Analyse

- Veranschaulichung und Untersuchung der Daten
- Intuitive Filter sollten vorhanden sein
- Forensische Analyse über einen Zeitraum
- Transaktions- und Verbindungsanalyse
- Deep Packet Inspection (DPI)
- Unterstützung für Decryption
- Analyse findet immer retrospektive statt
- Bemessung der Ursachen des Vorfalles
- Wirkungsweise des eingetretenen Vorfalls
- Rekonstruktion von Dokumenten und Bildern
- Analyse findet niemals am originären System statt!

Netzwerk Forensik – Aufbereitung und Präsentation

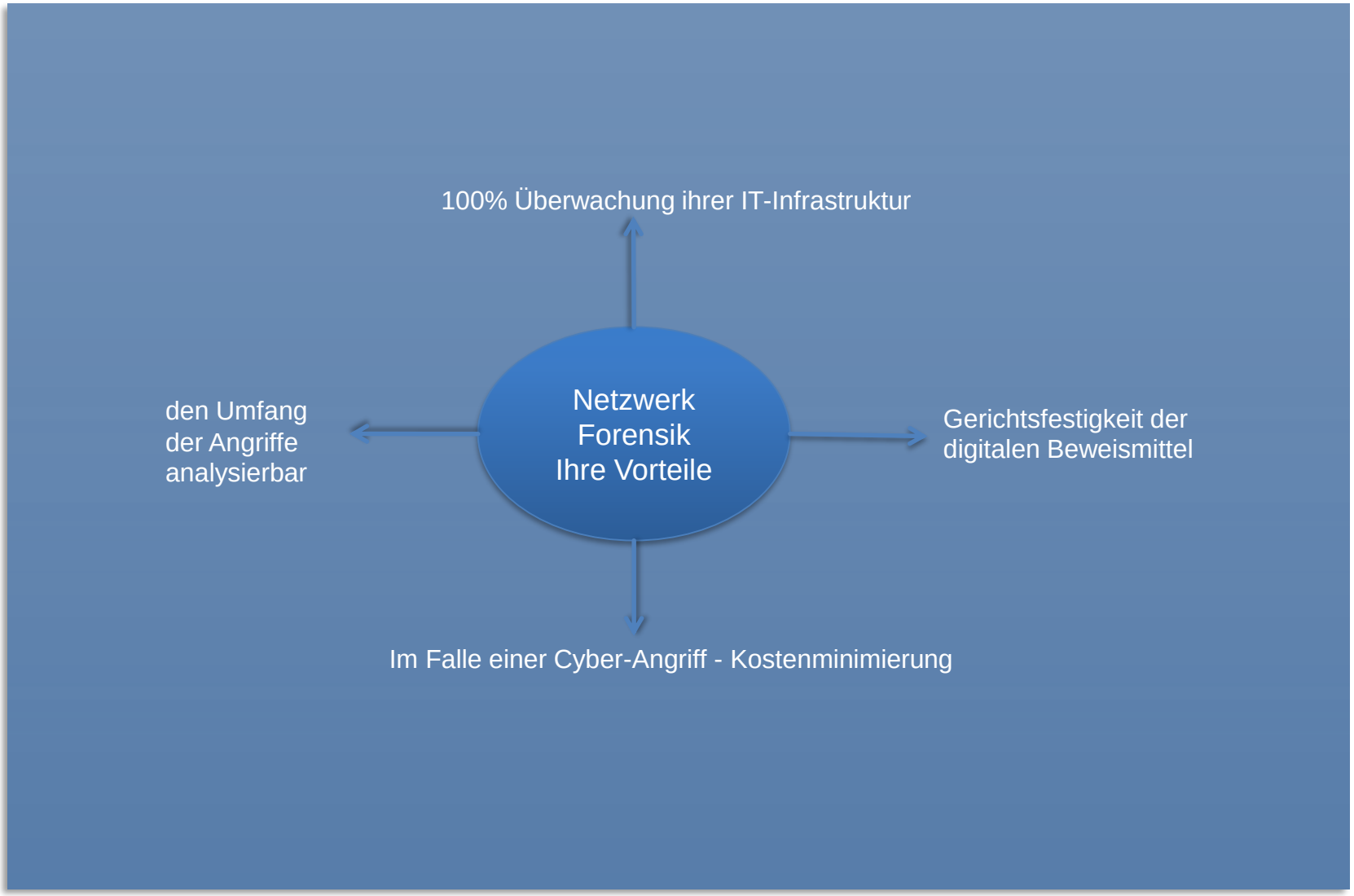
- Tatbestände werden in Form eines Berichts festgehalten

- Ermittlung der Identität des Täters / der Täter → Wer?
- Ermittlung des Zeitfensters der Tat (Erstellung einer Timeline) → Wann?
- Ermittlung des Umfanges der Tat → Wo?
- Ermittlung der Intension der Tat → Was?
- Ermittlung der Ursache und Durchführung → Wie?

Ob sich alles restlos klären lässt, ist abhängig vom vorhandenen Datenmaterial und von der Qualität der Analyse

Anforderungen an eine Netzwerk Forensik Lösung

- Datenaufzeichnung (Performance, Storage, transparent, unsichtbar)
- Datenaufbereitung (Daten filtern, aussortieren, indexieren)
- Datenanalyse (Anomalien und Erkennungsmuster erkennen)
- Vollständigkeit (Daten Integrität, Keine Paketverluste erlaubt, Line-speed aufzeichnen)
- Skalierbarkeit (1G, 10G, 40G, 100G, Mediatypen, Glasfaser, Kupfer)
- Flexibilität (Realtime und Offline Analysen)
- Verfügbarkeit (lückenlose Daueraufzeichnung, nicht angreifbar, keine IP Adresse)


100% Überwachung ihrer IT-Infrastruktur
den Umfang der Angriffe analysierbar
Netzwerk Forensik Ihre Vorteile
Gerichtsfestigkeit der digitalen Beweismittel
Im Falle einer Cyber-Angriff - Kostenminimierung

Daten/Fakten Zusammenfassung Netzwerk Forensik

- Lückenlose Sicherstellung von Beweisketten
- Analysen finden niemals auf Livesystemen statt
- Pakete lügen nicht!
- Risikominimierung/Kostenminimierung
- Bessere Kontrolle
- Klärung der wichtigsten Fragen (W-Fragen)

Vielen Dank für Ihre Aufmerksamkeit!

Timur Özcan

Tel: +49 6103 37 215 910
Mob: +49 173 36 24 983
timur.ozcan@neox-networks.com
www.neox-networks.com

Kontaktdaten:

NEOX NETWORKS GmbH
Otto-Hahn Straße 8
63225 Langen / Frankfurt am Main