T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2014
Berlin, 03. - 04.11.2014

Aktuelle Herausforderungen der IT-Forensic

Alexander Geschonneck
Partner, Head of Forensic, KPMG AG WPG

KPMG

cutting through complexity

Herausforderungen bei der Analyse großer Datenmengen

Alexander Geschonneck

Partner, Head of KPMG Forensic

Risiken

Es stellen sich verschiedene Fragen bezüglich Big Data und Sicherheit:

- Sind die Daten vertrauenswürdig?
- Sind die Daten ausreichend geschützt?
- Welche Daten kann man preisgeben ohne sich selbst zu schaden?
- Wie werden die Daten (weiter)verarbeitet?
- Wie können die Daten effektiv analysiert und ausgewertet werden?

KPMG

cutting through complexity

Daten, Daten, Daten

Herausforderungen

Herausforderungen bei der Analyse großer Datenmengen

Strukturierte Daten	Unstrukturierte Daten	Übergreifend
Daten, die strukturell gleichartig und regelmäßig aufgebaut sind Diese sind beispielsweise in ERP- oder CRM-Systemen, bzw. in Datenbanken jeder Art zu finden	Lose Daten ohne Regelmäßigkeit. Diese sind beispielsweise auf Laptops, PCs, Servern, Netzwerkumgebungen oder auf Smartphones oder Tablets zu finden	Verfahren und Themen, die gleichermaßen für jedwede Datenbestände relevant sind
■ ERP- & CRM-Systeme ■ Buchhaltungs- , Vertriebs- und Logistikdaten, … ■ Logfiles ■ Export & Verarbeitung ■ In Memory ■ Predictive Analytics	■ E-Mail Daten ■ CD, DVD, Blu-ray, Laptop, PC, etc. ■ Server (Sharepoint, Dateiserver) ■ Backup-Bänder ■ Mobile Devices	■ Anonymisierung ■ Skalierbarkeit ■ Archivierung

Forensische Datenanalyse – Was ist das?

Reaktiv / historisch

Proaktiv / vorausschauend

Deskriptiv

Was ist passiert?

Kontinuierliche Beobachtung

Was passiert gerade?

Prädiktiv

Was wird passieren?

Strukturierte Daten
Analyse strukturierter Daten

Strukturierte Daten (Datenbanken, Protkoll- und Logdateien)...

... ermöglichen die Erkennung von Wirtschaftskriminalität durch:

- forensische Plausibilisierung,
- Modellierung von Handlungsmustern,
- Analysen von Protokolldateien
- Überwachung von Key Fraud Indicators (KFI) und
- statistische Methoden.

...bieten die Möglichkeit, getrennte Datenbestände zusammenzuführen.

Die Methoden müssen häufig individuell erarbeitet werden und benötigen Erfahrung.

KPMG

cutting through complexity

Unstrukturierte Daten

Unstrukturierte Daten
Herausforderungen

Herausforderungen in Bezug auf große Datenmengen

1. Ständig steigende Datenmengen bis hin zu mehreren Terabytes
2. Unterschiedliche Datenquellen (Rechner, Server, Mobile Endgeräte etc.)
3. Unterschiedliche Datentypen
   (Office, Email, Audio, Instant Messages, SMS, Systemdaten, flüchtige Daten etc.)
4. Weltweit verteilte Custodians in unterschiedlichen Jurisdiktionen
5. Unterschiedliche Verfahren zur Datenidentifizierung und Sicherung notwendig (bitweise Kopien, logische Sicherung von ausgewählten Daten, vor Ort, remote, Datenübername
6. Erweiterung der Auswertungsbasis: Carving, Decryption
7. Unterschiedliche Verarbeitungsanforderungen durch unterschiedliche Jurisdiktionen bei einheitlichem Auswertungsziel (z. B. spezifische Datenexklusion und Anonymisierung)
8. Unterschiedliche Qualitätssicherungsanforderungen zur Gewährleistung von Vollständigkeit und Integrität
9. Unterschiedliche Verarbeitungszeiten bei einheitlicher Deadline
10. Konvertierung von bestimmten Daten aus Performancegründen und zur Gewährleistung einer Auswertung auf Basis eines einheitlichen reviewfähigen Formats

Unstrukturierte Daten
Vorbereitung

Anzahl von > 1.000.000 Emails pro Case inzwischen die Regel

Mailarchivaufbereitung und Extraktion

- Carving in lokalen Mailarchiven (PST, NSF, etc.) nach gelöschten Elementen
  - Mails im Papierkorb
  - "doppelt" gelöschte E-Mail (auch aus Papierkorb entfernt)
- Extraktion einzelner Elemente aus Mailarchiven
  - E-Mails
  - Kalendereinträge
  - Notizen
  - Attachments
  - Autovervollständigungslisten für E-Mailadressen – hat der Benutzer eine bestimmte E-Mailadresse eingegeben?

Unstrukturierte Daten
Vorfilterung (1/3)

Vorfilterung

Ziel: Kostenersparnis, Einhaltung Datenschutz

- Dateitypenfilter, Suchwortfilter, Zeitraumfilter
- (Filterung von als „privat“ etc. markierten Daten
  - Ordner „privat“
  - Markierung „privat“
  - Betreff „privat“)
- Filterung „Betriebsrat“ oder bspw. Kommunikation zwischen Eheleuten (wenn beide im Unternehmen sind) → Anwaltskommunikation (Attorney Client Privilege)

Unstrukturierte Daten
Deduplizierung und Early Case Assessment (1/2)

Deduplizierung

- Erkennung von gleichen Dokumenten
- Beispiel:
  - A sendet eine E-Mail an B und C
  - Mailbox von A und B wird in Reviewsoftware eingespielt
  - Dokument wird aufgrund von Deduplizierung nur einmal dargestellt (Information, dass E-Mail von A und B stammt wird dargestellt)
  - Mailbox von C wird im Nachgang eingespielt
  - E-Mail von C wird ebenfalls Dedupliziert

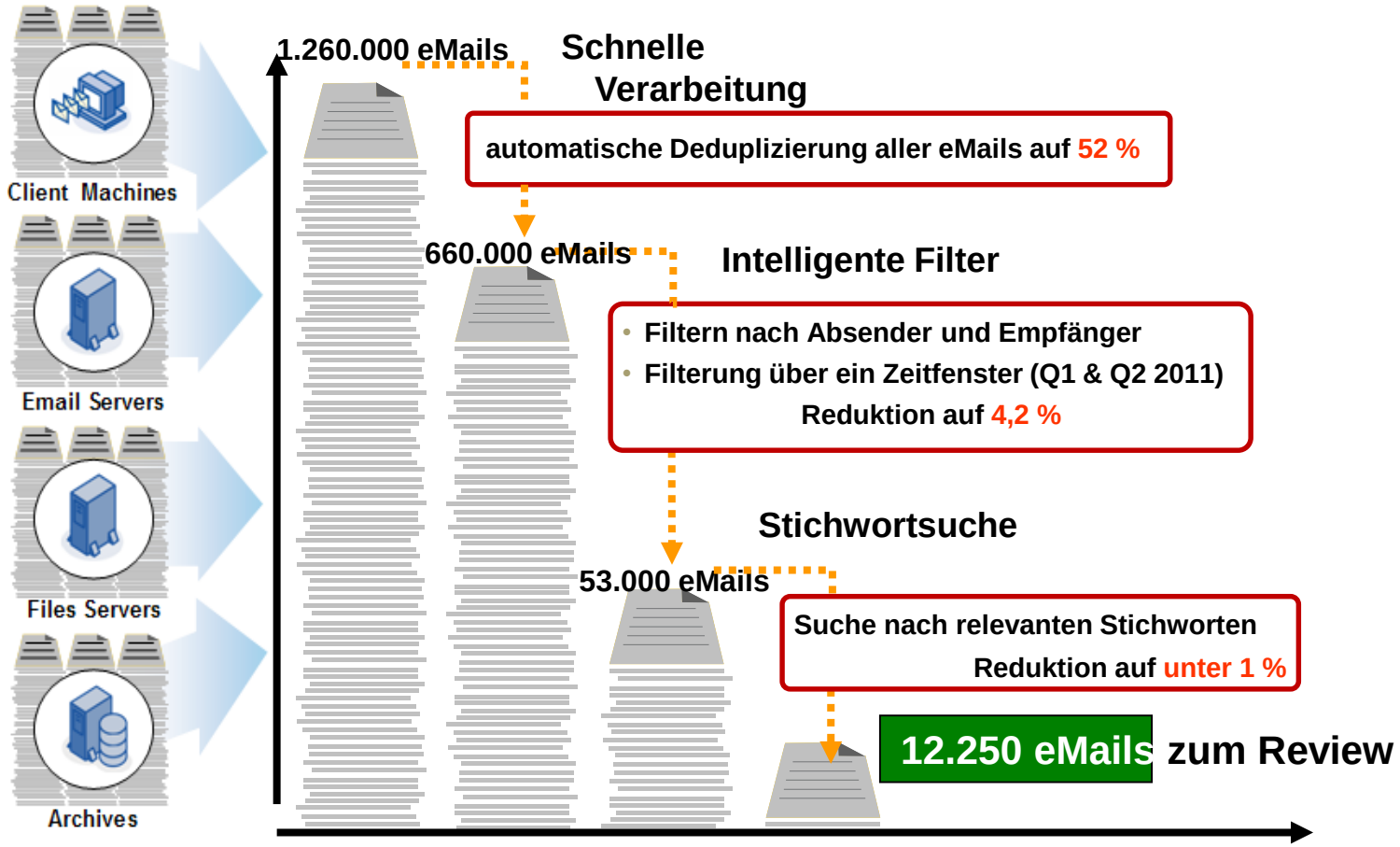
  Ziel: Kostenersparnis durch geringere Lizenzkosten und Zeitersparnis, Speicherplatz

Early Case Assessment

- Rasche, zielgerichtete Erstselektion der Daten die dem Review zugeführt werden
- Übersicht über erhaltene Datenmengen oder Kommunikationswege

Unstrukturierte Daten
Deduplizierung und Early Case Assessment (2/2)

Ausgangspunkt: 1.260.000 eMails gesichert und bereitgestellt



Unstrukturierte Daten
Early Case Assessment

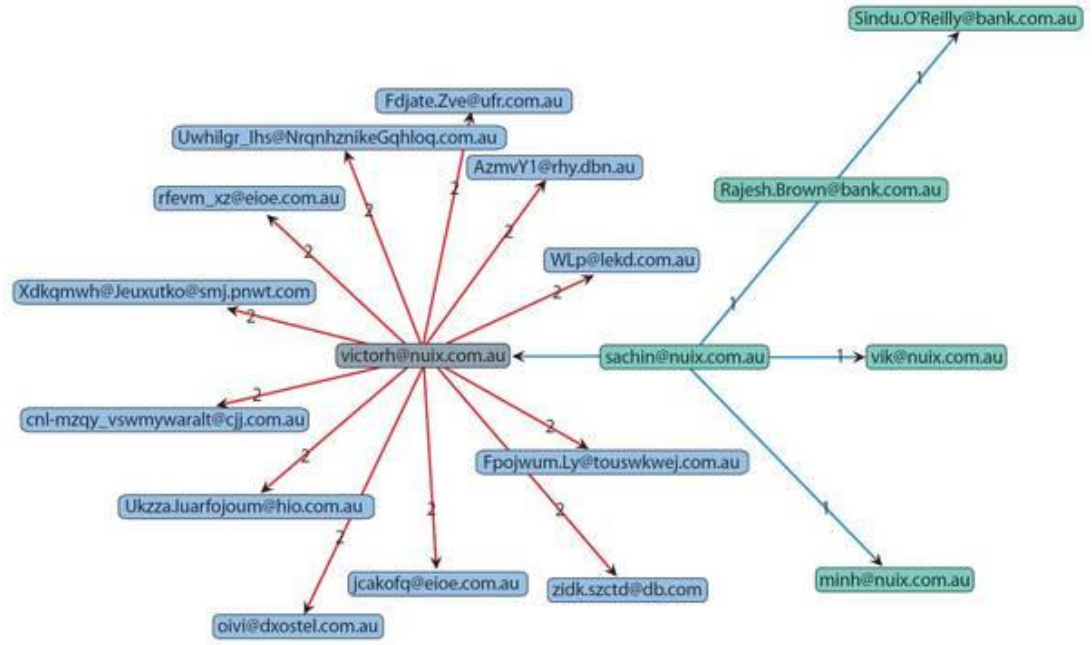
Suchwortlisten* (Standardsuchwortlisten ->Basis für die Erstellung fallbezogener Suchwortlisten

Verdächtiger Personenkreis

Untersuchungs-zeitraum

Filter

Selektion auf Basis grafischer Datendarstellung (E-Mail Kommunikations-Diagramm)



* Stammwortsuche

- Suche: Leben
- Gefunden: Leben, leben, lebt, lebte, gelebt, ableben, Lebensweisheit, erleben, Lebenszeit, etc.

KPMG

cutting through complexity

Vielen Dank!

KPMG

Alexander Geschonneck
Partner, Forensic

T +49 30 2068-1520
M +49 174 3201475
ageschonneck@kpmg.com

KPMG AG Wirtschaftsprüfungsgesellschaft,
eine Konzerngesellschaft der KPMG Europe LLP

KPMG

cutting through complexity

Vielen Dank für Ihre Aufmerksamkeit!

KPMG 24/7-Notruf-Hotline bei Verdacht auf Wirtschaftskriminalität und Cybercrime
Sie erreichen unsere Forensic-Experten rund um die Uhr telefonisch:

0180 KPMG FOR* (+49 1805 764367*)

*Telefonkosten: Festnetz 14ct/min; Mobilfunknetze 42ct/min

oder

http://kpmg.de/forensic

@KPMG_DE_FOR (https://twitter.com/KPMG_DE_For)