nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Vorbeugung ist die beste Medizin

… und was Sie im Ernstfall trotzdem tun können

06.03.2015

Martin Wundram
DigiTrace GmbH

Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen

DigiTrace
Kompetenz in IT-Forensik

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

Agenda

- 1. Was ist IT-Forensik?
- 2. Möglichkeiten der IT-Forensik
- 3. Vorbeugung ist die beste Medizin
- 4. Im Ernstfall
- 5. Fragen?

Begrüßung

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Über mich:

- Martin Wundram
- Diplom-Wirtschaftsinformatiker (Universität zu Köln)
- Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, insbesondere IT-Sicherheit und IT-Forensik
- Geschäftsführer der DigiTrace GmbH, TronicGuard GmbH
  - Standort Köln
    - 6 Personen im Team
    - Kunden von KMU bis DAX + Behörden

DigiTrace
Kompetenz in IT-Forensik

Begrüßung

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Meine Einschätzung:

- Ein Statement zu **IT-Forensik**:
  - Zu fast jedem Vorfall lassen sich sinnvolle Untersuchungen durchführen. Meist lassen sich dadurch Angriffswege/Hergänge nachvollziehen. Täter und betroffene Daten bleiben dabei jedoch häufig im Dunkeln. *Beteiligte IT-Systeme müssen zeitnah (oft sofort) angemessen berücksichtigt werden.*

DigiTrace
Kompetenz in IT-Forensik

Was ist IT-Forensik?

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

Foto (Menschen): andresr / Clipdealer
Foto (Evidencetüte): shawnhempel / Clipdealer
Foto (Zielscheibe): olivier26 / Clipdealer
Foto (TafelGrafikMitHand): convisum / Clipdealer
Foto (Lupe): stevanovicigor / Clipdealer

DigiTrace
Kompetenz in IT-Forensik

Was ist IT-Forensik?

- Storytelling
- **Abfluss vertraulicher Daten: Mitarbeiter wechseln mit Daten**
- Finanzieller Schaden: unbezifferbar, >25.000 EUR

Was ist IT-Forensik?

- Storytelling

Was ist IT-Forensik?

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

- Storytelling

DigiTrace
Kompetenz in IT-Forensik

Was ist IT-Forensik?

- Storytelling: Datenverlust mit (unnötigen) Folgeaktionen

Finanzieller Schaden: mindestens 300.000 EUR

Möglichkeiten der IT-Forensik

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Kurze Übersicht:

- Allgemein: Sicherung, Aufbereitung, Bereitstellung, Interpretation und Aufklärung digitaler Datenspuren aus IT-Systemen
- Beweissicherung (post mortem und live) und Beweismittelmanagement
- Erstellung von Gutachten / Sachverständigentätigkeit
- Bereitstellung aufbereiteter Daten für die Suche (e-Discovery)
- Auswertung von Massendaten
- Prävention (Forensic Readiness) und Compliance
- Beratung und Projektbegleitung
- Achtung: Datenschutz und andere rechtliche Hürden
- Achtung: Verschlüsselung, proprietäre Datenformate

DigiTrace
Kompetenz in IT-Forensik

Möglichkeiten der IT-Forensik

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Typische Herausforderungen / Fragestellungen:

- Gibt es Hinweise auf Straftaten oder fraudulente Aktivitäten (z.B. Wirtschaftskriminalität)? Welche?
- Störfall oder Sicherheitsvorfall? Wurde ein IT-System manipuliert?
- Welche Datenspuren stützen die eigene Position bei rechtlichen Auseinandersetzungen? Schadenerfassung und Schadenersatz?
- Gibt es auffällige Muster in Massendaten? Was kann daraus erkannt werden?
- Wie können in einer großen Menge elektronischer Daten schnell relevante Dokumente gefunden werden? Wie können diese Daten auch für Dritte durchsuchbar gemacht und bereitgestellt werden?

DigiTrace
Kompetenz in IT-Forensik

Vorbeugung ist die beste Medizin…

Wie können wir uns überhaupt noch schützen?

Vorbeugung ist die beste Medizin…

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

Grundsätzliche Überlegung

- Interagierende Systeme können in der Praxis nicht 100% sicher sein
- Mit der Annäherung an 100% steigt der Aufwand überproportional
- Einem großen Teil der Angriffsvektoren kann man jedoch bereits mit einfachen Maßnahmen begegnen – nur über solche werden wir im Folgenden sprechen

DigiTrace
Kompetenz in IT-Forensik

Vorbeugung ist die beste Medizin…

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Einfache Schutzmaßnahmen 1/5

- **Angemessenes Sicherheitsbewusstsein schaffen**
  - https://www.allianz-fuer-cybersicherheit.de
  - „Gewisse“ Webseiten haben öfter „Spezialfunktionen“
  - Im Zweifel lieber auf eine Software/App/Dienst verzichten
  - **Das Schutzbedürfnis der eigenen Daten erkennen**
  - …
- Stand der Technik an Schutzmaßnahmen einhalten
  - z.B. Virenscanner mit aktuellen Signaturen
  - Windows XP NICHT mehr verwenden
  - Updates (automatisch) installieren
  - Banking per HBCI
  - …

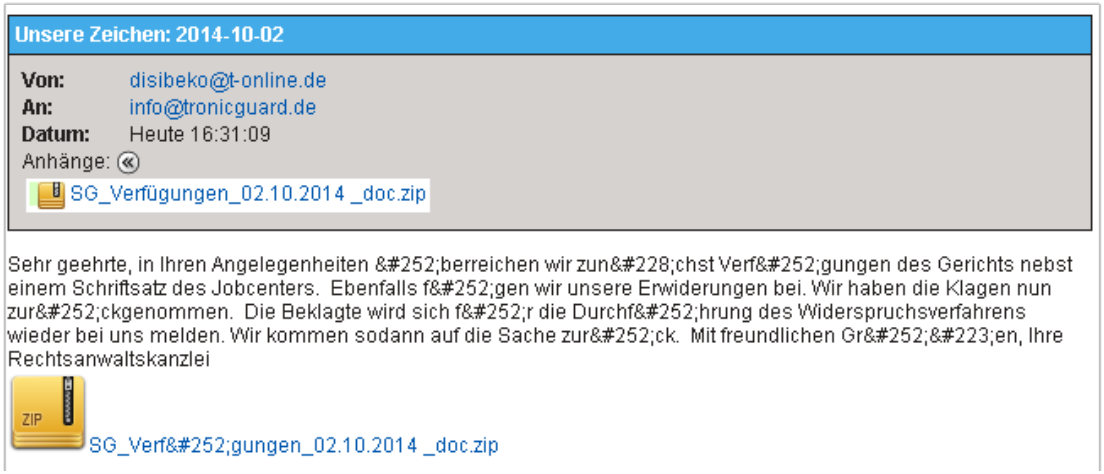
DigiTrace
Kompetenz in IT-Forensik

Vorbeugung ist die beste Medizin…

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Einfache Schutzmaßnahmen 2/5

- Nicht jedes dubiose Dokument öffnen



Unsere Zeichen: 2014-10-02

Von: disibeko@t-online.de
An: info@tronicguard.de
Datum: Heute 16:31:09
Anhänge:
SG_Verfügungen_02.10.2014 _doc.zip

Sehr geehrte, in Ihren Angelegenheiten überreichen wir zunächst Verfügungen des Gerichts nebst einem Schriftsatz des Jobcenters. Ebenfalls fügen wir unsere Erwiderungen bei. Wir haben die Klagen nun zurückgenommen. Die Beklagte wird sich für die Durchführung des Widerspruchsverfahrens wieder bei uns melden. Wir kommen sodann auf die Sache zurück. Mit freundlichen Grüßen, Ihre Rechtsanwaltskanzlei

ZIP SG_Verfügungen_02.10.2014 _doc.zip

DigiTrace
Kompetenz in IT-Forensik

Vorbeugung ist die beste Medizin…

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Einfache Schutzmaßnahmen 3/5

- Datenträger / vertrauliche Daten verschlüsselt sichern
  - Z.B. Festplattenvollverschlüsselung mit Windows Bitlocker und Bitlocker To Go
  - Oder TrueCrypt-Container verwenden (auch in der Cloud möglich)
  - Idealerweise auch E-Mail-Verschlüsselung verwenden
  - …
- Sicherungskopien ausreichend oft erstellen und sicher lagern
  - Welche Daten sind mir wie wichtig?
  - Einfach und komfortabel als „Basislösung“. Daten gelegentlich auf 2-3 USB-Festplatten auslagern
  - Sicherungsmedien am besten nicht im oder am PC lagern…
  - Gelegentlich prüfen, ob die Sicherungskopien auch noch funktionsfähig sind (insbesondere bei CD/DVD)

DigiTrace
Kompetenz in IT-Forensik

Vorbeugung ist die beste Medizin…

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Einfache Schutzmaßnahmen 4/5

- Alte Hardware und alte Datenträger sicher entsorgen
  - Mit der Bohrmaschine einmal durch die Festplatte bohren, oder mit dem Hammer auf die Controller-Platine hauen reicht für den „Hausgebrauch“, CD/DVD durchschneiden
  - Mobiltelefone „auf Werkseinstellung zurücksetzen“ als Mindestmaßnahme
- **Netzwerke segmentieren / trennen**
  - Nach Möglichkeit WLAN und LAN trennen, zumindest Gäste-Zugang trennen
  - **Unternehmen: eigenes Netzwerk für Internet, Trennung von wichtigen internen Daten**
- **Mehrere PCs / Smartphones für Aufgaben-/Funktionstrennung**

DigiTrace
Kompetenz in IT-Forensik

Vorbeugung ist die beste Medizin…

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Einfache Schutzmaßnahmen 5/5

- Sichere Passwörter, angemessenes Passwortmanagement
  - Heikles Thema!
  - Länge vor Komplexität
  - Unterschiedliche Passwörter verwenden, diese auch wechseln
  - Evtl. „Passwort-Safe“ verwenden
  - …
- Im Zweifel Expertenrat einholen
- *Denn: Im Bereich Informationssicherheit kann manchmal „ein falsches Bit“ zu massiven Sicherheitsproblemen führen*

DigiTrace
Kompetenz in IT-Forensik

Im Ernstfall… (als Privatperson)

Sofortmaßnahmen bei einem Störfall/Sicherheitsvorfall:

- besonnen, aber zügig reagieren
- Prüfen, ob alle wichtigen Daten in einem funktionsfähigen Backup vorhanden sind
- durchgeführte Schritte und Ereignisse bestmöglich dokumentieren, Gedächtnisprotokolle fertigen, Fotos machen
- Frühzeitig Expertenrat einholen (dies kann ein „normaler" IT-Administrator sein, möglicherweise sollte aber direkt ein „Facharzt" befragt werden)
- Www.botfrei.de und abwägen, ob eine Neuinstallation nötig ist
- Wenn das Smartphone abhanden gekommen ist: prüfen, ob Dienste/Accounts darauf abrufbar sind → evtl. sperren

Im Ernstfall… (als Unternehmen 1/2)

nrw·unITS
IT-Sicherheit
Nordrhein-Westfalen

Sofortmaßnahmen bei einem Störfall/Sicherheitsvorfall:

- besonnen, aber zügig reagieren
- klären, welche Personen als vertrauenswürdig und welche als möglicherweise im Fokus eingeschätzt werden (z.B. IT-Administratoren?)
- möglichst keine Aufregung im Unternehmen erzeugen, nur erforderlichen vertrauenswürdigen Personenkreis und nur im erforderlichen Umfang einweihen
- sich der Domäne IT aktiv stellen (nicht erst Akten wälzen, Interviews führen und das Problem vertagen)
- wenn möglich, Geräte/Daten, Sicherungsmedien sofort einfordern/sicherstellen
- Daten nicht verändern, bitte keine eigene Aufklärung auf den Originaldaten, nur auf Kopien

DigiTrace
Kompetenz in IT-Forensik

Im Ernstfall… (als Unternehmen 2/2)

Sofortmaßnahmen bei einem Störfall/Sicherheitsvorfall:

- durchgeführte Schritte bestmöglich dokumentieren, Gedächtnisprotokolle fertigen
- Szenarien entwickeln für verschiedene Fälle: Wie soll man reagieren, falls sich herausstellt, dass …
- Priorität des Falles festlegen und entsprechend behandeln
- internen / externen Sachverstand heranziehen, ggf. Krisenreaktionsteam: IT-Forensiker rechtzeitig einbinden/anfragen
- rechtzeitig weitere zu Beteiligende einbeziehen (z.B. Legal, Datenschutzbeauftragter, Betriebsrat) und rechtliche Fragen klären (lassen)
- Bei IT-Outsourcing: rechtzeitig externe Dienstleister anfragen

Welche Fragen haben Sie?

Autor:
Martin Wundram/ Geschäftsführer

E-Mail:
wundram@digitrace.de

Unternehmen:
DigiTrace GmbH
Zollstockgürtel 59
50969 Köln

Web:
www.digitrace.de.de

Vielen Dank für Ihre Aufmerksamkeit!

nrw·unITS IT-Sicherheit Nordrhein-Westfalen

Ministerium für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen

DigiTrace Kompetenz in IT-Forensik

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds für regionale Entwicklung