Forensic Readiness

FH Aachen: 9. IT-Forensik Workshop – 12.06.2019

Kurzvorstellung

PERSON

- **Martin Wundram**
- Jahrgang 1982
- Diplom Wirtschafts-informatik, Uni Köln

wundram@digitrace.de

ERFAHRUNG (AUSWAHL)

Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, **insbesondere IT-Sicherheit und IT-Forensik**

Lehrbeauftragter der Universität zu Köln

Geschäftsführer und Gründer der DigiTrace GmbH

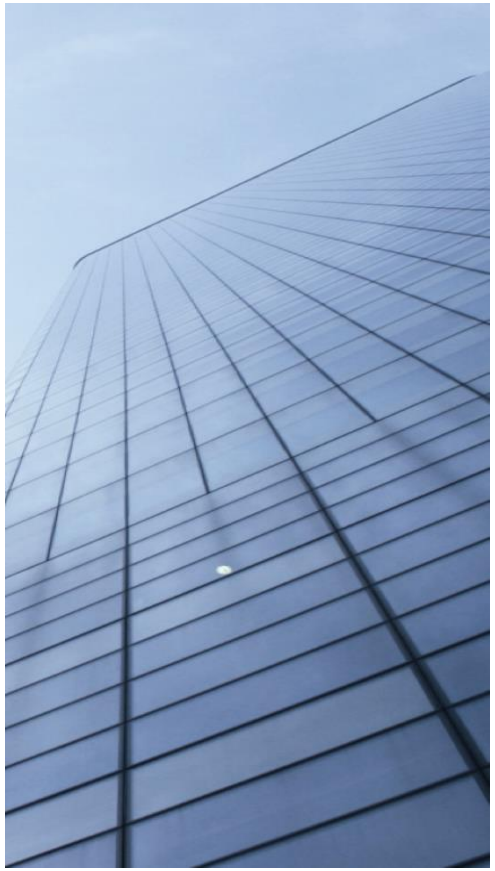
Teamgröße am Standort Köln: 5 IT-Forensiker + 2 weitere Mitarbeiter

Kunden von KMU bis DAX + Behörden

- Präventive Projekte: Audits, Penetrationstests, IT-Sicherheitskonzepte, strategische Beratung zu IT-Sicherheit, …
- Reaktive Projekte: IT-Forensik, Incident Response, eDiscovery, …
- Sachverständigentätigkeit / Gutachten zu allen Themen der IT

Agenda

1	Storytelling
2	Grundlagen
3	Rechtliche Einschränkungen
4	Typische Fehler und Lösungen
5	Fazit und Rückblick
6	Fragerunde und Ausblick

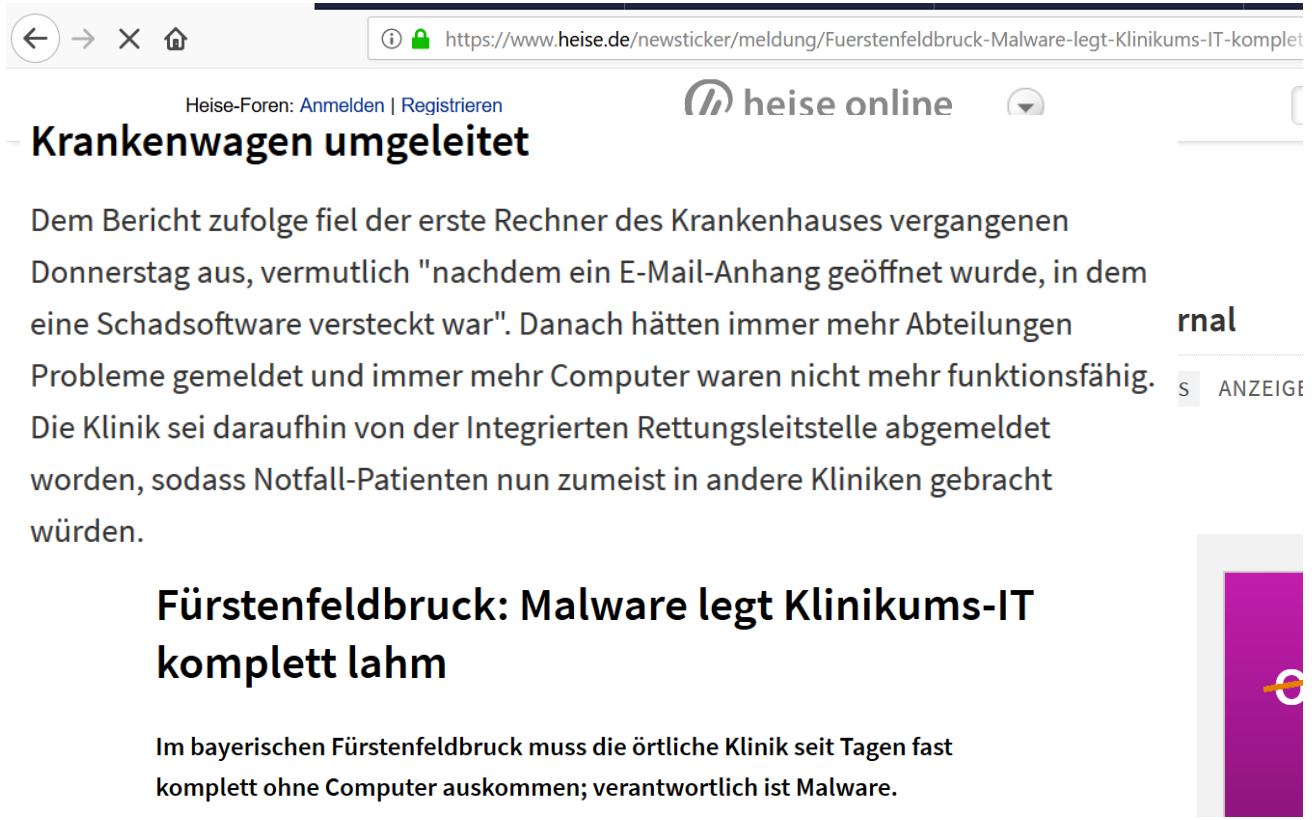


Storytelling

Standardschadsoftware legt Klinik lahm

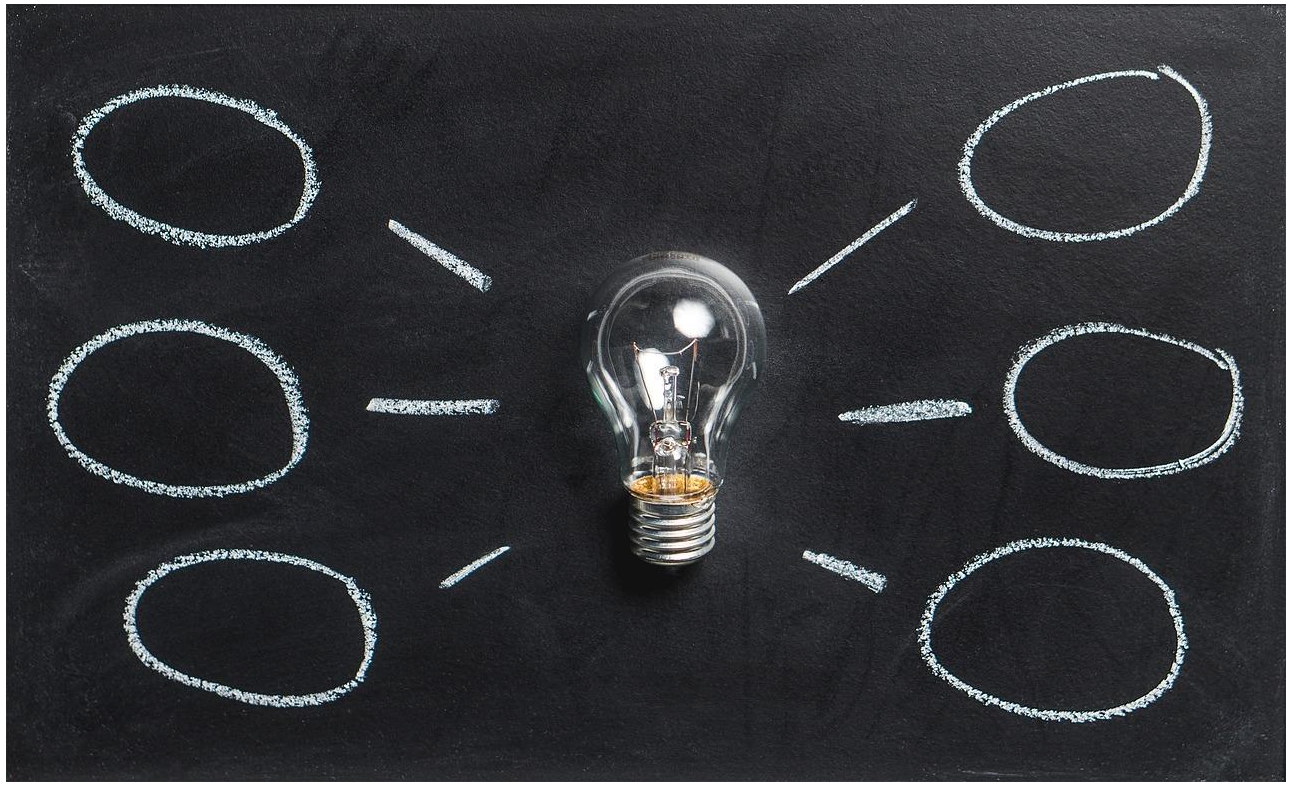
Ihre Meinung:

- gut, mittel, schlecht reagiert?



Grundlagen

Was ist Forensic Readiness für Sie?



Grundlagen

Was ist Forensic Readiness (laut Literatur)?

- ***„die Maximierung der Verarbeitungsfähigkeit digitaler Beweise bei gleichzeitiger Minimierung der Ermittlungskosten“***
  (frei übersetzt nach Robert Rowlingson, “A Ten Step Process for Forensic Readiness”, International Journal of Digital Evidence Winter 2004, Vol. 2, Iss. 3)

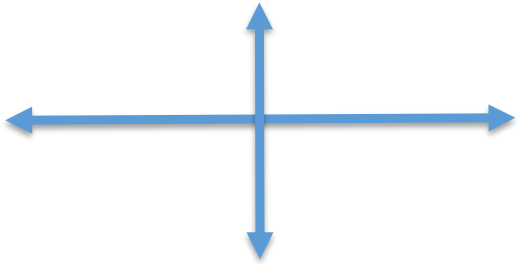
- ***„Erreichen eines angemessenen Niveaus an Fähigkeiten durch eine Organisation, damit diese in der Lage ist, digitale Beweise zu erheben, zu bewahren, zu schützen und zu analysieren. Zweck: diese Beweise in Rechtssachen, insbesondere in Disziplinarangelegenheiten, vor einem Arbeitsgericht oder Gericht wirksam verwenden können“***
  (frei übersetzt nach CESG Good Practice Guide No. 18, Forensic Readiness)

Grundlagen

Herausforderungen aus Sicht des Geschäftsführers

Juristische Herausforderungen

Interne / taktische Herausforderungen



Finanzielle Herausforderungen

Technische Herausforderungen

Grundlagen

Was ist IT-Forensik?

Häufiger Fokus: wer hat was wann (warum) gemacht

Menschen <-> Daten

Grundlagen

Was ist IT-Forensik?

Totforensik (post mortem)

Live-Forensik

Netzwerkforensik

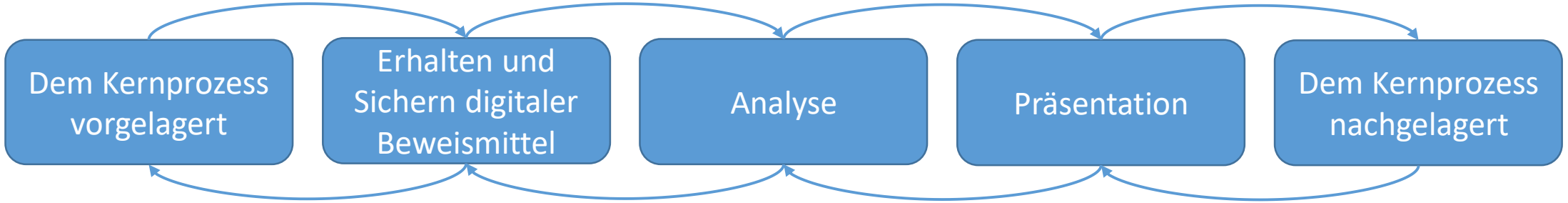
Sachverständigengutachten

eDiscovery

Sicherheitsvorfall

Datenabfluss

Compliance-Verstoß



Grundlagen

Was ist IT-Forensik?

- Exkurs: Locard‘sche Regel / Locard‘sches Prinzip

- Kontakt zwischen zwei Objekten (Täter, Opfer, Tatort, …) nicht möglich ohne wechselseitige Spuren
- Gilt in der Praxis auch in der IT:
  - Täter hinterlässt Logdatei-Einträge
  - Täter löscht Logdatei, hinterlässt aber gelöschte Datei im Dateisystem
  - Täter überschreibt Datei vorher, hinterlässt dadurch aber wieder Einträge in anderer Logdatei
  - …

Grundlagen

Was ist ein Sicherheitsvorfall?

- Mögliche Definitionen

- **Ereignis**: Auftreten eines beobachtbaren Geschehens, typischerweise zeitpunktbezogen und Differenz von Vorher/Nachher
- **Vorfall/Incident**:
  - **(Technischer) Störfall**: Störung des bestimmungsgemäßen Betriebs einer technischen Anlage (Verweis auf „Fehler“)
  - **IT-Sicherheitsvorfall**: ungesetzliche, nicht autorisierte oder einfach unerwünschte Handlung unter Beteiligung eines IT-Systems

- Störfall oder Sicherheitsvorfall?
- Festplatte geht durch Verschleiß kaputt vs. Innentäter sabotiert IT, tritt gegen Server

Grundlagen

Achtung:

- IT-Forensik ist nicht nur bei IT-Sicherheitsvorfällen notwendig

- (anlassunabhängige) Compliance-Prüfungen
- Fraud Investigation (Schmiergeldzahlungen, Betrugsversuche)
- Unterstützung von Insolvenzverwaltern
- …

- Daher: Forensic Readiness ist nicht nur als präventive Maßnahme gegen IT-Angriffe („Hacker“) wichtig und notwendig

Grundlagen

Was ist Incident Response?

- Strukturierte und koordinierte Vorgehensweise ausgehend von der Vorfallerkennung bis zur Lösung

- Kernaktivitäten:
  - Untersuchen und Einschätzen, ob Sicherheitsvorfall oder nicht
  - Details zum Incident herausfinden, Schadenseinschätzung
  - Schadenminimierung, Notfallmaßnahmen
  - Übergang zum Normalbetrieb
  - PR
  - Lessons Learned, Systemhärtung

Grundlagen

Ziele können sich ergänzen oder gegenseitig behindern

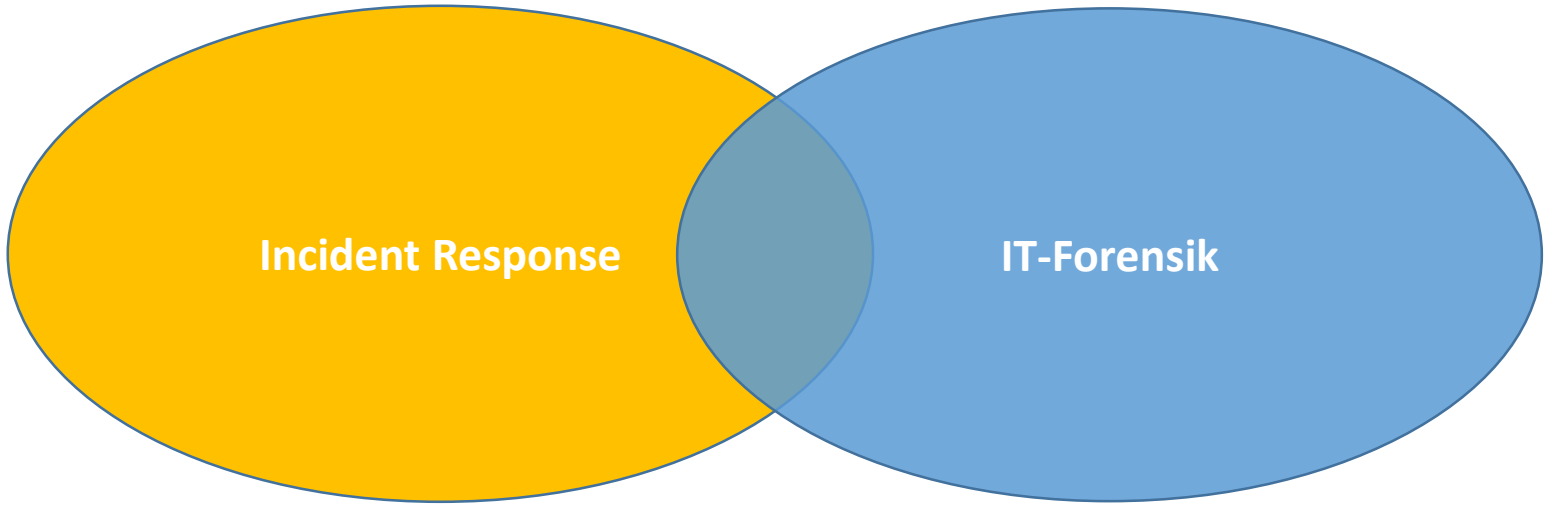
- Angriff stoppen oder laufen lassen?
- Zukünftige Angriffe verhindern?
- Täter finden?
- Hergang aufklären?
- Mitarbeiter einbeziehen oder auslassen?
- Ermittlung/Strafverfolgung einbeziehen?
- Priorisierung?
- Systeme abschalten oder laufen lassen?
- Offen oder verdeckt ermitteln?

Verantworten muss letztlich der Geschäftsführer

Grundlagen

Schnittmenge und Abgrenzung

- Hauptunterschied: Zielsetzung



Grundlagen

Was ist ein CERT/CSIRT?

- CERT – Computer Emergency Response Team
- CSIRT – Computer Security Incident Response Team

- existieren als externe Organisationen (etwa CERT-Bund, CERT/CC)
- zunehmend auch unternehmensintern

- Digitale „Ersthelfer“ bis hin zu erfahrenen IT-Forensikern
- Mitglieder beschäftigen sich vollständig oder zu einem signifikanten Teil ihrer Zeit mit der IT-Sicherheit des Unternehmens
- Aufgabe: Sicherheitsvorfälle bewältigen, koordinieren, aber auch vermeiden

Grundlagen

Was ist Compliance?

- „Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien“ (Deutscher Corporate Governance Kodex)

- je nach Unternehmensgröße gibt es dafür eigene Abteilungen
- Verstöße erkennen, abstellen und damit Schaden vom Unternehmen abwenden
- Aufgabe vergleichbar mit der eines CERTs, aber auf regulatorischer Ebene

- Sowohl CERT/CSIRT als auch Compliance sind typische Auftraggeber von externen IT-Forensikern

Grundlagen

Welche Regelwerke können bei der Entwicklung von Forensic Readiness unterstützen?

- Zahlreiche Normen/Frameworks und weitere Dokumente existieren, hier nur einige für den Vortrag besonders relevante:

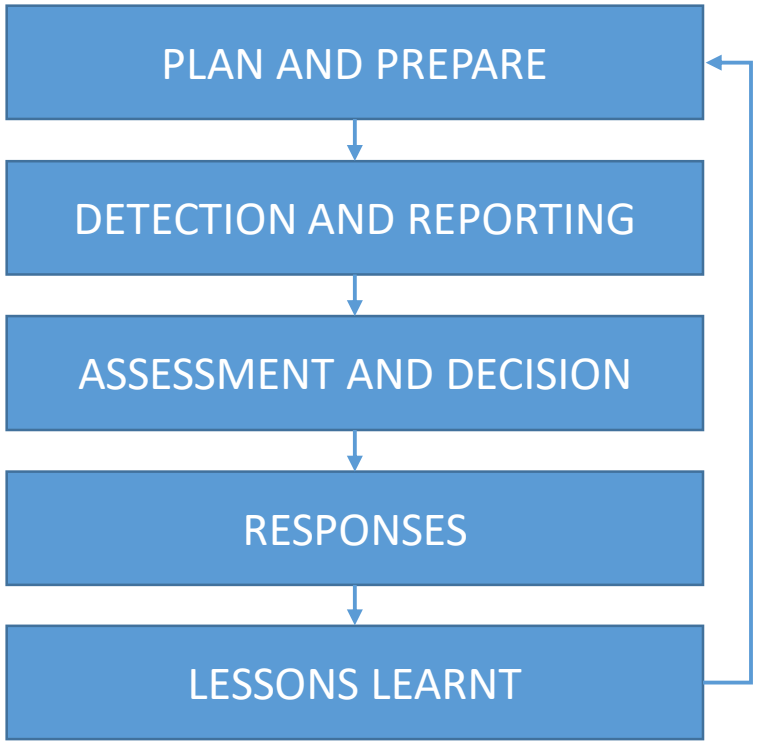
- ISO/IEC 27035-1
- ISO/IEC 27035-2
- BSI-Standard 100-4 (Notfallmanagement) (bzw. Nachfolgestandards 200-x)
- BSI-Leitfaden IT-Forensik

Grundlagen

ISO/IEC 27035-1 und ISO/IEC 27035-2

- Part 1: Principles of incident management
- Part 2: Guidelines to plan and prepare for incident response

- Fokus im Bereich IT-Sicherheitsvorfall
- Insbesondere Teil 2: Vorbereitung
  - Erstellung von Policies
  - Erstellung eines Incident Management Plans
  - Vorlagen zur Vorfallsdokumentation
  - Verortung im Unternehmenskontext



Grundlagen

BSI-Standard 100-4

- „Notfallmanagement“ (aktuell noch weiter gültig)

- Beschreibt Maßnahmen um auf Krisen aller Art reagieren zu können
- Ziel: Notfallbewältigung und Geschäftsfortführung (Business Continuity)
- Gehört numerisch in die Reihe der (alten) IT-Grundschutz-Standards (100-1 bis 100-3), versteht sich aber als eigenständig

[…]
5.1 Die Business Impact Analyse
5.2 Risikoanalyse
5.3 Aufnahme des Ist-Zustandes
5.5 Notfallvorsorgekonzept
[…]

viele wichtige Aspekte, die für Forensic Readiness übernommen werden können

Grundlagen

Goldener Tipp

- Schablone zum Melden von Ereignissen
- In der Vergangenheit z.B. von DigiTrace erstellt

2. Event Number		**Incidents** (if applicable)	
4. Reporting Person Details			
4.1 Name		4.2 Address	
4.3 Organization & Department		4.4 Phone Number & E-Mail-Address	
5. First Responder (IT)			
5.1 Name		5.2 Address	
5.3 Organization & Department		5.4 Phone Number & E-Mail-Address	
6. Information Security Event/Incident Description			
What? How? Why? Initial views on components/assets affected Adverse business impacts identified vulnerabilities			
7. Information Security Incident Details (only applicable if Event escalated to Incident)			
7.1 Date & Time the incident occurred		7.2 Date & Time the Event Incident was discovered	
7.3 Date & Time the incident was reported		7.4 If the Incident is over, how long did it last?	
8. Category	Actual / Suspected Incident		
8. Category (cont.)			

Grundlagen

BSI-Leitfaden IT-Forensik

- Grundlagen- und Nachschlagewerk

- praxisbezogen
- erklärt, was IT-Forensik ist, wie sie in Unternehmensprozesse eingebettet werden kann, wie vorgegangen wird, was erwartet werden kann, …
- gibt auch praktische Erläuterungen zu einzelnen forensischen Artefakten
- Problem: Technik schreitet rasant voran, Leitfaden ist von 2011:
  - „Die grundlegende Methode ‚Betriebssystem‘
  - – Das Betriebssystem MS Windows XP“

- Wichtig: Grenzen/Einschränkungen der genutzten Ressourcen müssen klar sein

Grundlagen

Gutachten 1/2

- Begründetes Urteil eines Sachverständigen über eine Zweifelsfrage. Es enthält Darstellungen von Erfahrungssätzen und die Ableitung von Schlussfolgerungen für die tatsächliche Beurteilung eines Geschehens oder Zustands durch einen oder mehrere Sachverständige.
- Sie geben dem Gericht (oder einem sonstigen Auftraggeber) die notwendige Sachkenntnis für einen bestimmten Sachverhalt
- In einem Gutachten muss der Sachverständige darlegen, was er als gegeben annimmt und wie er zu seinen Ergebnissen kommt
- Nur dann ist das Gericht (bzw. der Auftraggeber) in der Lage, das Gutachten zu überprüfen und sich das erforderliche eigene Bild von der Richtigkeit der vom Sachverständigen gezogenen Schlüsse zu machen.

Grundlagen

Gutachten 2/2

- Ein Gutachter ist bei der Gutachtenerstellung grundsätzlich „frei“
- Klare Vorgaben, dass nach bestimmten Standards BSI / NIST vorzugehen ist, existieren grundsätzlich nicht (abgesehen z.B. von der Sachverständigenordnung für öbuv-Sachverständige).
- Jedoch kann es sich vor Gericht negativ auswirken, wenn nicht sachgerecht die Beweise gewonnen wurden / das Gutachten nicht nach den anerkannten Regeln der Technik erstellt wurde.
- Lücken im Gutachten können sich negativ auswirken und Schadensersatzforderungen nach sich ziehen…

Grundlagen

Gutachter und Sachverständige

- „eine Person, die auf einem bestimmten Gebiet der Geistes- oder Naturwissenschaften, der Wirtschaft, der Technik oder eines anderen Sachgebietes überdurchschnittliche Kenntnisse und Erfahrungen hat und diese Sachkunde in Ausübung eines Gewerbes oder eines freien Berufes jedermann persönlich, unparteiisch, unabhängig und objektiv zur Verfügung stellt“, Ulrich, Der gerichtliche Sachverständige
- Gutachter und Sachverständiger können synonym verwendet werden
- Wer kann Sachverständiger sein? Wer kann nicht Sachverständiger sein?
- Unterscheidung zwischen Privatgutachter und gerichtlichem Gutachter
- Stets eine natürliche Person. Kann aber in einer Organisation tätig sein, z.B. in einem akkreditierten Labor
  -> Berufung vs. Beauftragung
- Problem: evtl. Besorgnis der Befangenheit
- Entscheidet ein Sachverständiger? Richtet er über Schuld und Unschuld?
- Ist ein IT-Sachverständiger noch objektiv, wenn er nach seiner Unterstützung in Incident Response auch noch das IT-Gutachten für ein Gericht erstellt?

Grundlagen

Erstellung von Gutachten durch private Sachverständige

- Berufsrecht öbuv- und ISO 17024-zertifizierter Sachverständiger
- Verankerung in StPo § 73 Auswahl des Sachverständigen und ZPO § 404 Sachverständigenauswahl
- Ein öffentlich bestellter und vereidigter Sachverständiger ist zur gewissenhaften Erfüllung seiner Obliegenheiten öffentlich verpflichtet. Dies ist ähnlich einer Beleihung.
- Er unterliegt einem Begutachtungszwang und wird von Gerichten „entschädigt“
- Aufträge können sich auf drei Bereiche beziehen:
  - Mitteilung von Erfahrungssätzen
  - Tatsachenfeststellung
  - Beurteilung von Tatsachen
- Analog: Wirtschaftsprüfer
- Ist Beweismittel, wenn vom Gericht beauftragt. Privatgutachten hingegen sind „lediglich“ (qualifizierter) Parteivortrag (oder Zeuge im Strafverfahren)

Rechtliche Einschränkungen

- Ermittlungsmaßnahmen bzw. Maßnahmen, bei denen (private) IT-Forensiker involviert sein können, stellen oftmals einen Eingriff in Grundrechte des Betroffenen dar:
  - Menschenwürde
  - Datenschutz
  - Fernmeldegeheimnis
  - Schutz des Eigentums
  - …
- Je intensiver der Eingriff, desto höher die Anforderungen an die Rechtfertigung

Rechtliche Einschränkungen

Wer hat welche Befugnisse?

- staatliche Ermittlung

- Umfassende Befugnisse:
  - Durchführung von Durchsuchungen
  - Beschlagnahme von Beweismitteln
  - Überwachung (TKÜ, Wohnraumüberwachung, …)
  - Vernehmung von Beschuldigten oder Zeugen
  - …

Rechtliche Einschränkungen

Wer hat welche Befugnisse?

- private Ermittlung
- „Der Gesetzgeber behandelt den Privatermittler wie jeden Privatmann, d.h. es gibt keine hoheitlichen oder quasi-hoheitlichen Rechte zur Vornahme von vertraglich vereinbarten Ermittlungsmaßnahmen“ (Grüner, Der Ermittlungsauftrag durch Unternehmen zur Überwachung von Mitarbeitern und Organen)

- **Keine Befugnis, Zwangsmaßnahmen anzuwenden, etwa wegen eines Verdachts zum Zwecke einer Untersuchung die Datenverschlüsselung eines Mitarbeiters ohne dessen Zustimmung zu überwinden -> Gefahr der Strafbarkeit eigener Handlung**
- Notwehr, Nothilfe gelten grundsätzlich, aber: besondere Stellung eines externen IT-Forensikers als „Profi“
- Besonders „brisant“: Geheimes/verdecktes Vorgehen – mögliche Strafbarkeit des Ermittlers inkl. zivilrechtliche Schadensersatzklagen usw. (Haftung)!

- Deshalb: für eine Untersuchung sollte im Idealfall die Einwilligung des Betroffenen vorliegen!

Rechtliche Einschränkungen

Wer hat welche Befugnisse?

- Einwilligung durch Betroffene

- grundsätzlich zwei Varianten möglich:
  - Einwilligung vor dem Vorfall, etwa durch Betriebsvereinbarungen, IT-Richtlinien, …
  - Einwilligung nach dem Vorfall und bezogen auf den jeweiligen Einzelsachverhalt:
  - „Erklären Sie sich damit einverstanden, dass wir Ihr (auch) dienstlich
  - verwendetes iPhone auswerten? Bitte stellen Sie uns dieses zur
  - Verfügung und teilen uns auch den PIN zum Entsperren mit.“
  - Alternativ: mit Rechtsbeistand prüfen, ob/wie Maßnahmen ohne Einwilligung möglich sind

Rechtliche Einschränkungen

Verwertbarkeit

- Belastbar ist nur das, was auch legal ist. Bedeutung für (gerichtliche) IT-Gutachten?
  - bei der Erstellung müssen alle technischen und rechtlichen Implikationen beachtet werden
  - Legal = Einhalten des Rechtsrahmens -> IT-Forensik = Recht + IT
- „Gemähte Wiese“
  - Wenn einmal ermittelt wurde, gibt es u.U. nicht mehr viel zu ermitteln
  - Alles muss „sauber“ ablaufen
  - Oft kein zweiter Versuch, bzw. Risiko der eingeschränkten Verwertbarkeit

Rechtliche Einschränkungen

Verwertbarkeit

- Stichwort „Write-Blocker“
- Ist ein Gutachten belastbar, wenn Write-Blocker verwendet wurden?
- Ist es nicht belastbar, wenn sie nicht verwendet wurden?
  - „ein Neurochirurg arbeitet doch auch ohne „Write-Blocker“
  - Live-Forensik…
- Welchen Stellenwert hat ein Write-Blocker für ein Gutachten?
- Welchen Stellenwert haben IT-Werkzeuge generell?

Rechtliche Einschränkungen

Verlässlichkeit

- Produkt A (Web-History-Tool): ~30% der Firefox-History (SQLite-Datenbank!) wurden kommentarlos übersehen
- Produkt B (Standard-Suite): „Fehler 42 in Komponente XY bei Auswertung MFT. OK klicken für Weitermachen“ → großer Teil der Dateien wurde nicht angezeigt, unter anderem die Outlook-.PST mit entlastenden Spuren!
- Produkt C (Live-Forensik-Tool): Reproduzierbarer Absturz bei Sicherung des DNS-Cache, weitere Auswertung nicht möglich
- Produkt D („Mächtiges“ Artefakt-Tool): Neueste Version findet in eigenem Case-Dataset von älterer Version plötzlich eine Vielzahl neuer protokollierter Webseitenaufrufe
- Produkt E (Anti-Forensik- / Datenlöschungs-Tool): Wurde verwendet, um Spuren gründlich zu vernichten, hat aber innerhalb einer SQLite-Datenbank nicht alle Einträge überschrieben, sondern einzelne Einträge „übersehen“

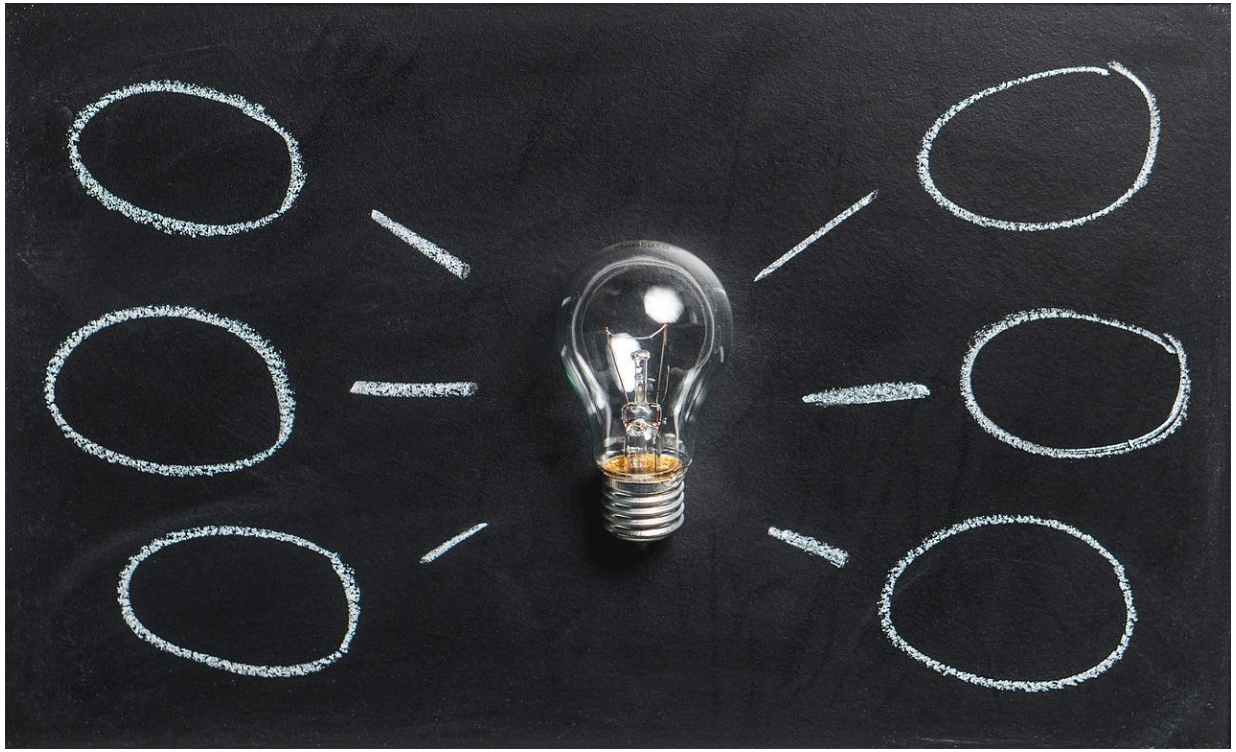
Rechtliche Einschränkungen

Tretminen (Beispiel)

- IT-Forensik durch privaten IT-Forensiker
- Auftraggeber ist ein Unternehmen, dass das Notebook eines tatverdächtigen Mitarbeiters untersuchen lassen möchte + Erstellung eines Gutachtens
- Ein Rechtsanwalt verwendet das Gutachten in einem Zivilprozess gegen diese Person
- Der Angeklagte behauptet später, diese Daten könnten gar nicht vor Gericht verwendet werden. Vielmehr habe sich der IT-Forensiker bei der Datengewinnung selbst strafbar gemacht, weil:
  - Der fragliche Rechner sei sein Privatrechner, nicht sein Dienstrechner
  - Die Festplatte sei verschlüsselt gewesen, insbesondere sei ein bestimmtes Verzeichnis passwortgeschützt gewesen. Der IT-Forensiker habe also StGB § 202a (1) verletzt, denn er habe eine Passwortsicherung widerrechtlich überwunden
- Dies konnte jedoch erfolgreich widerlegt werden:
  - Belege aus dem Unternehmen, dass doch dienstlicher Rechner (vorsorglich durch den IT-Forensiker bereits bei der Sicherung erhoben)
  - Nachweis: Der sogenannte Passwortschutz war nicht wirksam, es bedurfte daher keiner Überwindung

Typische Fehler und Lösungen

Was denken Sie?



Typische Fehler

1. Sicherheit wurde in der IT-Landschaft bisher noch gar nicht berücksichtigt.
2. Auf einem Server wird Schadsoftware gefunden. Es ist völlig unklar, was für Auswirkungen dies haben könnte. Es gibt keinerlei Informationen über den Server und dessen Verwendung im Unternehmen. Altlast? Kundendaten?
3. Mitarbeiter erhält eine E-Mail und öffnet die vermeintliche Rechnung im Anhang. Ein schwarzes Fenster erscheint, der Mitarbeiter traut sich nicht, dies der IT mitzuteilen.
4. Ein Unternehmensstandort verfügt nicht über lokale IT-Kräfte. Auch während der Incident Response kümmert sich niemand darum, diesem Standort verlässlich Kräfte zuzuweisen. Es entsteht/bleibt ein „Vakuum“.

Typische Fehler

5. Der IT-Forensiker muss im Ortstermin mehrere Stunden warten, da sich die Rechtsabteilung noch nicht sicher ist, ob die Untersuchung des fraglichen Laptops überhaupt zulässig ist.
6. Die Incident Response in einem großen Unternehmen erfolgt unkoordiniert, der CIO ist implizit verantwortlich, aber hat eigentlich überhaupt keine Zeit. Kommunikation erfolgt nur per Telko und per E-Mail. Niemand dokumentiert übergreifend und zentralisiert.
7. Der IT-Forensiker bekommt zum Ortstermin keine IT-Dokumentation. Nach dem Login auf ein System stellt er fest, dass der PC zwei IP-Adressen hat; offenbar stecken zwei Netzwerkkabel. IT-Administrator kann auf Rückfrage keine Antwort geben: „das hat mein Vorgänger gemacht“.

Typische Fehler

8. Es werden einfach immer komplette VMs auf ein NAS gesichert. Im Zuge eines zielgerichteten Angriffs vernichten die Täter auch alle für sie remote erreichbaren Backups. Es gibt nun keinerlei Datenbestände mehr…
9. Ein Backup existiert zwar, für dieses muss aber eine gesonderte rechtliche Genehmigung eingeholt werden (Funktionsänderung der Daten).
10. Logins von Benutzern können nicht mehr nachvollzogen werden, da der zu untersuchende Zeitraum drei Monate zurückliegt. Der Domaincontroller speichert seine Logdateien aber nur für zwei Stunden.
11. Der Auftraggeber ist völlig schockiert, als der IT-Forensiker ihm mitteilt, dass die Sicherung von drei 2 Terabyte-Platten und einem Mobilgerät ca. einen Arbeitstag dauert. Er beauftragt nicht und will den Fall aussitzen.

10-Punkte-Plan

Ein Vorschlag für bessere Forensic Readiness

1. Prävention
2. Bedarf festlegen und Szenarien entwickeln
3. Awareness
4. Rechtliche Absicherung
5. Partner suchen
6. Planung zukünftiger IT-Forensik-Einsätze
7. IT-Dokumentation pflegen
8. Datensicherungen berücksichtigen
9. Konfiguration der IT
10. Re-Evaluation

10-Punkte-Plan

1. Prävention

- **Ein hohes Maß an Sicherheit (IT-Sicherheit und physische Sicherheit) im Vorfeld hilft,**
  - **Vorfälle zu vermeiden**
  - **die Aufklärung durchzuführen**

- Hohe Hürden machen es „Neugierigen“ und „echten“ Angreifern schwerer
- Gelebte Sicherheitskultur hemmt „neugieriges Stöbern“ von Mitarbeitern
- Durchdachte Maßnahmen im Vorfeld sorgen für solide Spurenlage im Schadensfall

10-Punkte-Plan

2. Bedarf festlegen und Szenarien entwickeln

Szenarien ermitteln, die erwartbar auftreten können

- **Schutzbedarf festlegen (Vertraulichkeit, Integrität, Verfügbarkeit)**
- Nicht jedes Unternehmen muss die gleichen Vorfälle erwarten
- Grundsätzlich aber gewisse Szenarien erwartbar:
  - IT-Sicherheitsvorfall auf Client / Server („Hacking“/Schadsoftware)
  - Verdacht des Datenabflusses
  - Verdacht auf illegale Absprachen (PC „nur“ als Spurenträger)
  - …
- Daraus ableiten: was kann man tun, um solche Szenarien im Vorfeld abzumildern / die Aufklärung zu erleichtern?

10-Punkte-Plan

3. Awareness

Bei allen (!) Mitarbeitern Awareness (Situationsbewusstsein) für den Umgang mit Vorfällen schaffen

- Anwender: Bewusstsein dafür, wie ein Vorfall erkannt und gemeldet werden soll
- IT: Bewusstsein dafür, was ein Störfall ist und was ein Sicherheitsvorfall sein könnte; richtigen Eskalationsweg kennen
- Verantwortliche: Bewusstsein dafür, welche Ereignisse eine IT-forensischen Aufklärung benötigen; erwartbare Ergebnisse kennen

Sinnvoll: „Ersthelfer“-Rollen benennen, die speziell geschult werden

10-Punkte-Plan

4. Rechtliche Absicherung

Rechtliche Grundlagen schaffen bzw. den Ist-Zustand verbindlich klären

- Rechtliche Grundlage der eigenen Datenverarbeitung
- IT-Richtlinien, die erlaubte Nutzung von Systemen definieren
- Verträge mit IT-Dienstleistern auf Unterstützung bei IT-forensischen Untersuchungen prüfen
- Achtung: Betriebliche Anweisungen müssen für eine Wirksamkeit auch „gelebt“ werden (betriebliche Übung)
- Betriebsrat einbinden!

Wichtig: dies ist ein Thema für Volljuristen und andere juristische Experten!

10-Punkte-Plan

5. Partner suchen

Bereits im Vorfeld einen vertrauenswürdigen Partner für IT-forensische Maßnahmen suchen (+ Partner für weitere Gebiete, etwa PR)

- Im Ernstfall soll es schnell gehen können, ohne langwierigen Abstimmungsprozess
- Vertrauen ist bei so sensiblen Tätigkeiten besonders wichtig
- Ein passender Dienstleister ist kurzfristig möglicherweise schlecht oder gar nicht verfügbar (kein „Guter-Kunde-Bonus“)

Sinnvoll: Rahmenvertrag schließen, der die wichtigsten Aspekte bereits vorab klärt

10-Punkte-Plan

6. Planung zukünftiger IT-Forensik-Einsätze

Möglichkeiten und Anforderungen von IT-Forensik verstehen und umsetzen

- Ziel: Konkreten Auftrag im Ernstfall klar und passgenau formulieren können
- Klare Ziele setzen
- Realistische Erwartungen an Machbarkeit/technische Anforderungen stellen
- Eigene Verantwortlichkeiten verstehen und zeitnah erfüllen können
- Kommunikations- und Datenwege vorab planen/überdenken
- Notwendige Ressourcen bedenken und eventuell vorhalten (Lager-/Arbeitsraum? Datenträger? Testsysteme?)
- …

10-Punkte-Plan

7. IT-Dokumentation pflegen

Aktuelle, vollständige Dokumentation der eigenen IT-Landschaft vorhalten

- Externer Forensiker muss sich innerhalb kürzester Zeit vorbereiten / zurecht finden können
- Welche Systeme existieren?
- Welche Systeme wurden an welchen Mitarbeiter ausgegeben?
- Wie sind die Konfigurationen?
  - Hardware (spezielle Datenträger, die „exotische“ Adapter erfordern?)
  - Software (Verschlüsselung, RAID, administrative Beschränkungen der Geräte?)

10-Punkte-Plan

8. Datensicherungen berücksichtigen

Backups / Datensicherungen auch als forensisches Mittel einsetzen

- Backups, etwa von Logdateien, erlauben Blick weiter in die Vergangenheit zurück
- Funktionsdefinition als forensisches Mittel bereits zum Anlegen der Sicherung erleichtert die rechtliche Situation (keine Funktionsänderung)
- Speicherung von Logdateien in separatem System erhöht Manipulationssicherheit
- Ideal: Backups so managen, dass diese auch vertrauenswürdig genug sind und nicht manipuliert/sabotiert werden können (z.B. geschützte Lagerung)

10-Punkte-Plan

9. Konfiguration der IT

IT-Systeme derart konfigurieren, dass sie die Aufklärung unterstützen

- Zeitstempel auf allen Systemen synchronisieren (Zeitleiste/Korrelation): NTP
- Was wird wie und wie lange geloggt? -> Einstellungen passend wählen!
- Zuordenbarkeit einzelner IP-Adressen zu IT-Systemen
- Konfiguration separater Accounts pro natürlicher Person, die ein System verwendet (Single User Accounts)
- Eventuell Logs bereits mit Entstehung zentral sichern
- Schadsoftware nicht löschen, sondern in „Quarantäne“ verschieben
- …

10-Punkte-Plan

10. Re-Evaluation

Forensic Readiness ist ein lebender Prozess und muss stets angepasst werden

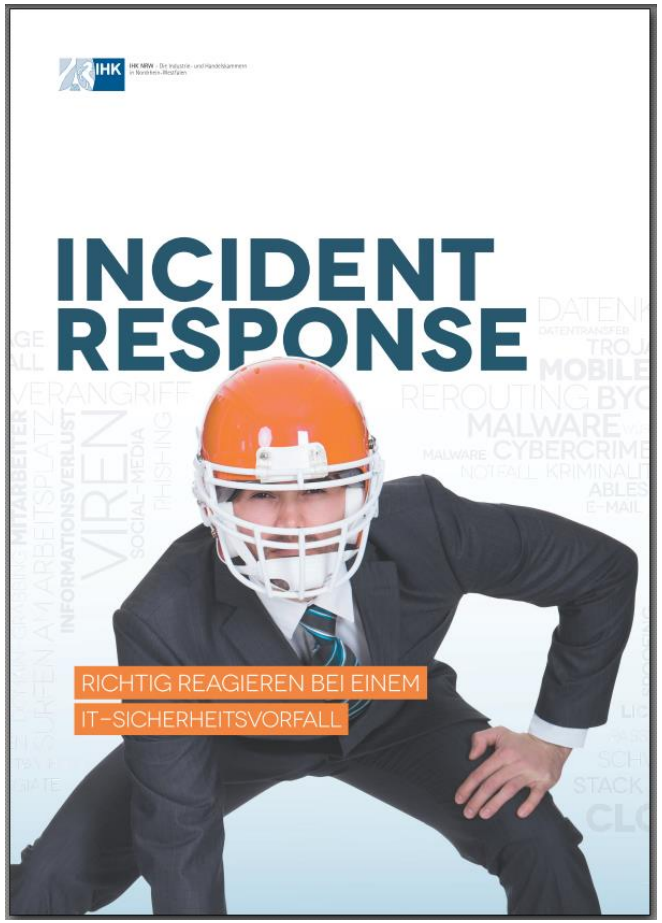
- Neue Technik sorgt für neue Herausforderungen, aber auch Möglichkeiten
- Neue Rechtsgrundlagen erfordern neue Bewertungen
- Unternehmen verändern sich stetig, bestehende Prozesse müssen angepasst werden
- Lessons Learned aus bewältigten Vorfällen ableiten

Sinnvoll: Regelmäßige Überprüfung fest in ein eigenes Forensic-Readiness-Konzept einplanen

Die Rolle des „Digitalen Ersthelfers“

- Typisches Profil: IT-erfahren oder sogar IT-Experte, aber kein Experte für IT-Forensik und Incident Response
- Wichtigste Tätigkeiten:
  - IT Incidents bemerken
  - Erhalten und je nach Situation, Ausrüstung und Erfahrung auch Sichern digitaler Beweismittel
  - Hinzuziehung von IT-Forensikern koordinieren
- Je nach konkreter Rollenbeschreibung:
  - Fall abgeben an IT-Forensiker, oder
  - Fall koordinieren und als Bindeglied zwischen Unternehmen und beauftragtem IT-Forensiker fungieren

Leitfaden Incident Response



DEFINITION

IT-SICHERHEITSVORFALL (INCIDENT)

Ereignis analog einem Notfall, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen, für welche Sie einen hohen oder sehr hohen Schutzbedarf definiert haben, in Ihrem Unternehmen / Ihrer Organisation derart beeinträchtigt, dass ein großer Schaden für Ihr Unternehmen / Ihre Organisation / Ihre Kunden oder Geschäftspartner entstehen kann.

RICHTIG REAGIEREN BEI EINEM IT-SICHERHEITSVORFALL

Bewahren Sie Ruhe und lassen Sie den Ernst der Lage prüfen. Egal ob ein „unachtsamer Klick" oder ein fortgeschrittener IT-Angriff - nur mit Ihrer rechtzeitigen Unterstützung und Mitarbeit können interne oder externe Experten den Fall aufklären und lösen.

Die nachfolgende Liste soll Ihnen helfen, bei einem möglichen IT-Sicherheitsvorfall bestmöglich zu handeln. Wir empfehlen Ihnen daher, diese Liste sofort greifbar aufzubewahren.

1. Reagieren Sie überlegt aber zügig. Erzeugen Sie möglichst keine Aufregung im Unternehmen. Weder auf die lange Bank schieben noch Panik sind gute Lösungen.
2. Prüfen Sie welche Personen vertrauenswürdig oder vorein-genommen sind bzw. möglicherweise im Fokus stehen. Holen Sie dann Expertenrat ein. Qualifizierte Fachexperten sollten rechtzeitig eingebunden werden. Bilden Sie gegebenenfalls ein Krisenreaktionsteam. Sorgen Sie für eine verlässliche Unterstützung durch Ihren externen Dienstleister.
3. Priorisieren Sie Ihr weiteres Vorgehen und weihen Sie nur erforderliche und vertrauenswürdige Personen ein.
4. Stellen Sie wenn möglich betroffene Geräte, Daten und Backups sicher. Prüfen Sie, ob alle wichtigen Daten in einem funktionsfähigen Backup vorhanden sind. Achten Sie auf die Vollständigkeit, Aktualität und Integrität der Daten. Lassen sich gesicherte Daten wirklich öffnen und zurückspielen?
5. Wenn das Smartphone oder ein anderes Mobilgerät abhand-engekommen ist, prüfen Sie, ob verbundene Dienste oder Accounts abrufbar sind und sperren Sie diese bei Bedarf.
6. Verändern Sie die Daten nicht, um keine Spuren zu verwi-schen. Arbeiten Sie stattdessen mit geeigneten (forensi-schen) Kopien.
7. Dokumentieren Sie den Vorfall sorgfältig. Protokollieren Sie dazu durchgeführte Schritte und Ihre Beobachtungen um-fangreich und genau, z.B. durch Fotos und exakte Zeitangaben.

   Beispiel: Am 01.04. um ca. 14:30 Uhr habe ich eine E-Mail mit einem angehängten Lieferschein erhalten. Die ZIP-Datei habe ich geöffnet, aber nicht gespeichert. Es öffnete sich kurz ein schwarzes Fenster. Ansonsten ist nichts passiert. Am darauf folgenden Tag konnte ich keine Word-Dateien mehr öffnen. Auf meinem Bildschirm erschien eine Warnung des FBI bezüglich illegaler Aktivitäten mit einer Zahlungsauffor-derung zwecks Strafe. Anbei befindet sich ein Foto von der Warnung, das ich mit meinem Handy erstellt habe.
8. Entwickeln Sie unterschiedliche Szenarien:
   - Wie reagiert man auf einen Innentäter?
   - Wie reagiert man darauf, wenn Kundendaten in fremde Hände geraten sind?
   - Wie lassen sich verlorene Daten wiederherstellen?
   - Was ist, wenn die eigenen IT-Systeme nicht mehr vertrauenswürdig sind?

„Better safe than sorry – Ein Fehlalarm ist besser als ein übersehener Sicherheitsvorfall."

EINFACHE PRÄVENTIVE MASSNAHMEN

Am besten sind Sie gut vorbereitet! Dazu hilft ein aktueller und vollständiger Infrastrukturplan (Was steht wo, Netzwerkplan, Konfiguration), ein Incident Response Plan (Liste zum „Abarbeiten" für den Ernstfall) und die präventive Kontaktaufnahme mit Ihren IT-Dienstleistern. Erar-beiten Sie mit diesen gemeinsam einen (kleinen) Plan, der die wichtigsten Punkte und Maßnahmen kurz skizziert.

https://www.ihk-koeln.de/upload/IHK_Leitfaden_Incident_Response_DINA4_05_54030.pdf

Goldene Tipps für den Ernstfall

- [x] Prüfen Sie, wer vertrauenswürdig ist
- [x] Priorisieren Sie das weitere Vorgehen
- [x] Arbeiten Sie forensisch „sauber“
- [x] **Gehen Sie von Anfang an koordiniert vor**
- [x] **Dokumentieren Sie den Vorfall genau**
- [x] Binden Sie relevante Personen ein
- [x] Stellen Sie ein Krisenteam zusammen
- [x] Entwickeln Sie verschiedene Szenarien

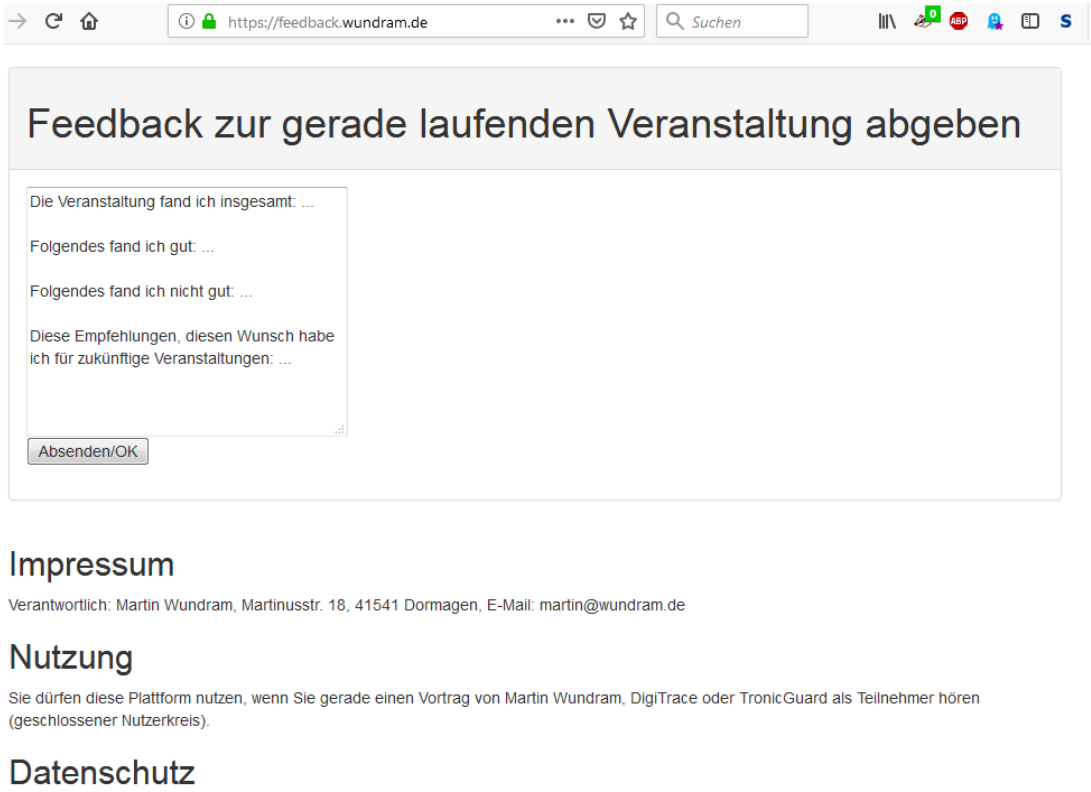
Fazit

- **Forensic Readiness und praktische Erfahrungen aus der Forensik sind komplex**: heute nur eine Einführung in die wichtigsten Aspekte und Fallstricke
- **IR und FR sind individuell**: während ein Unternehmen seine geheimsten Produktionszeichnungen schützen muss, ist für ein anderes Unternehmen ein langfristiger Ausfall der Produktionskette das schlimmste Szenario
- **Forensic Readiness zahlt sich aus**: die eigene Erfahrung des Vortragenden zeigt, dass immer wieder wertvolle Zeit verloren geht und vor allem, dass essenzielle Spuren mit besserer Vorarbeit auswertbar gewesen wären
- **Recht-technisch**: es ist wichtig, vorab juristische und technische Aspekte gemeinsam zu betrachten
  -> Interdisziplinär: Geschäftsführung, IT, Compliance, …

Fragerunde und Ausblick

WICHTIG: Feedback geben

- Bitte geben Sie konstruktives Feedback!
- Nur so können wir Ihre Erwartungen auch zukünftig bestmöglich erfüllen
- Anonymes Feedback-System: https://feedback.wundram.de



Fragerunde und Ausblick

Fragen

&

Antworten

Gerne auch im Nachgang an

Wundram@digitrace.de