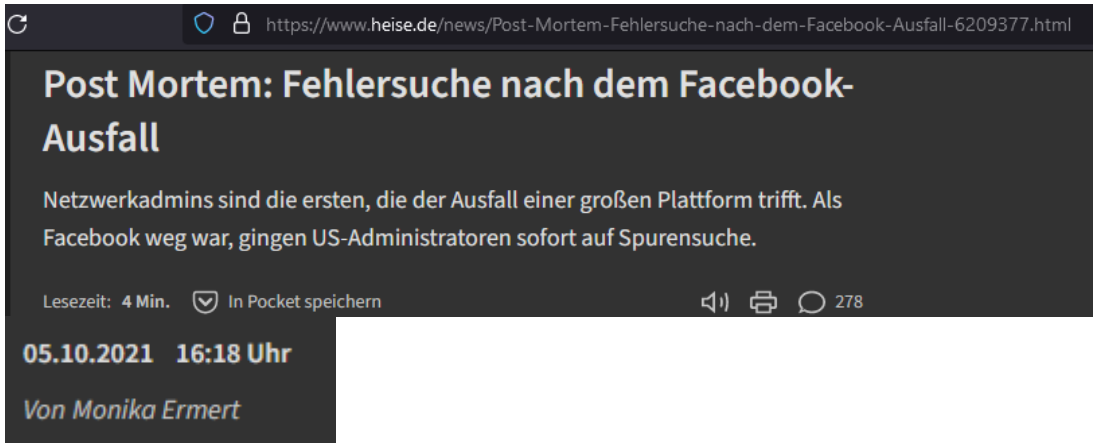
Mit dem „digitalen Ersthelfer“ besser auf erste IT-Fälle reagieren – Nutzen und Chancen zum Einsatz

It-sa, Nürnberg – 23.10.2024

Jeder verliert die Kontrolle


https://www.heise.de/news/Post-Mortem-Fehlersuche-nach-dem-Facebook-Ausfall-6209377.html

Post Mortem: Fehlersuche nach dem Facebook-Ausfall

Netzwerkadmins sind die ersten, die der Ausfall einer großen Plattform trifft. Als Facebook weg war, gingen US-Administratoren sofort auf Spurensuche.

Lesezeit: 4 Min. In Pocket speichern 278

05.10.2021 16:18 Uhr

Von Monika Ermert

Facebooks Zentralisierung der eigenen Infrastruktur führte offenbar zu einer verheerenden Kettenreaktion. Auf Twitter machten Meldungen die Runde, dass Facebook-Mitarbeiter nicht mehr ins Büro konnten, weil auch die vernetzte Schließanlage nicht mehr funktionierte. Schlimmer: Die Facebook-Administratoren konnten Medienberichten zufolge nicht auf die betroffene Hardware zugreifen, weil der Remote-Zugriff ohne Routen nicht funktionierte. Zugleich sollen die Mitarbeiter im Rechenzentrum nicht die nötigen Berechtigungen und Zugangsdaten gehabt haben, um die Routingtabellen direkt vor Ort zu reparieren.


https://www.heise.de/news/Nacktscanner-Unbedachte-Fotos-vom-Kind-fuer-den-Arzt-Goog

Missbrauchsverdacht: Intimfotos vom Kind für den Arzt – Google-Dienste gesperrt

In den USA haben Eltern Zugang zu allen Google-Diensten verloren, weil sie Fotos vom Genitalbereich ihrer Kinder für eine Vorabdiagnose an Ärzte gesendet haben.

Lesezeit: 3 Min. In Pocket speichern 564

22.08.2022 08:41 Uhr

Von Martin Holland

In einem Fall verlor der Vater nicht nur den Zugriff auf seinen Mail-Account und sein komplettes Adressbuch, sondern auch alle Fotos, mit denen er das erste Lebensjahr seines Sohnes dokumentiert hatte, schreibt die US-Zeitung. Weil er auch seinen Handyvertrag über Google abgeschlossen hatte, musste er sich nicht nur einen neuen zulegen. Ohne den Zugang zu seiner alten Handynummer habe er sich auch nicht mehr in andere Internetdienste einloggen können. Alles in allem sei er von einem Großteil seines digitalen Lebens ausgesperrt worden. Der zweite Vater, dessen Erlebnisse zusammengefasst werden, sei gerade dabei gewesen, ein Haus zu kaufen. Als sein Gmail-Account gesperrt worden sei, habe das zu Problemen mit dem Makler geführt.

Vorstellung von und Arbeit mit Fallbeispielen

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

Vorstellung von und Arbeit mit Fallbeispielen

Digitale Ersthilfe: Definition

- **Digitale Ersthilfe**:
  - Maßnahmen, die von einer als Digitaler Ersthelfer ausgebildeten Person umgesetzt werden, um im Sinne einer Ersthilfe auf einen möglichen Digitalen Ernstfall sowie auf „Hilferuf“ von Dritten mit ersten Maßnahmen zu reagieren.

- Der Begriff **Digitaler Ernstfall** (auch: **Digitaler Notfall**) soll wie folgt verstanden werden:
  - Ein IT-Sicherheits-Event oder IT-Sicherheit-Incident mit möglicherweise oder bereits festgestellt erheblichen Konsequenzen für Personen oder Organisationen.
- Analogie zur medizinischen Ersthilfe

Vorstellung von und Arbeit mit Fallbeispielen

BSI: Alarmstufe Rot -> Exchange/Hafnium im März 2021

- BSI meldet wiederholt (verschiedene Medienkanäle)
- Kunden erkennen Ernst der Lage, manche melden sich präventiv
- BSI / Microsoft stellen Detektierungsmöglichkeiten bereit
- „Regelbetrieb nicht mehr aufrecht erhaltbar“ → das gilt auch bei den IT-Sicherheitsdienstleistern

Vorstellung von und Arbeit mit Fallbeispielen

In drei einfachen Schritten zur Katastrophe

1. Alltäglicher Defekt an einem wichtigen Server inkl. Datenverlust
2. Das Backup wurde falsch konfiguriert – es wurde täglich nur ein leerer Ordner gesichert…
3. Aufgrund eines bestehenden Versicherungsschutzes wurde eine extrem teure Datenrettung beauftragt (x00.000 EUR)

Ergebnis:

- Versicherung möchte nicht zahlen (verständlich)
- Dienstleister wird in Regress genommen (x00.000 EUR, verständlich)
- Dienstleister ist insolvent

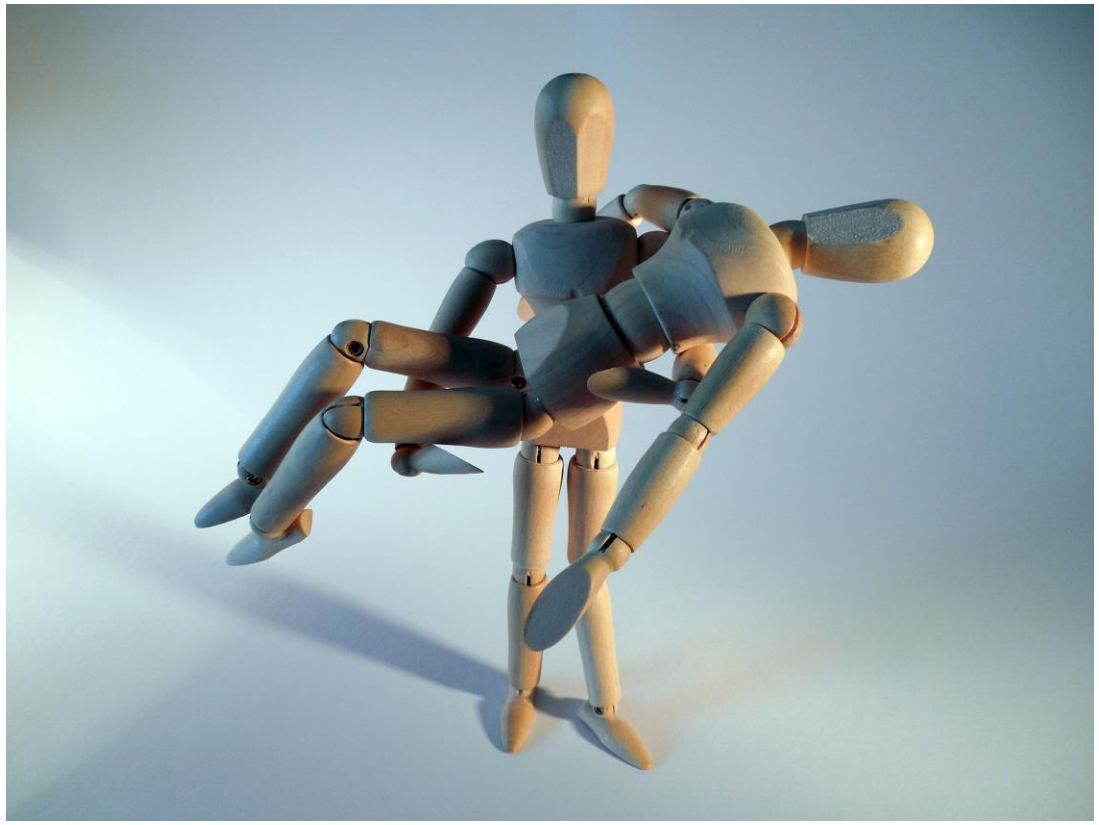
Vorstellung von und Arbeit mit Fallbeispielen

Jämmerlicher Umgang mit Meldungen von Dritten

Vorstellung von/Arbeit mit Fallbeispielen

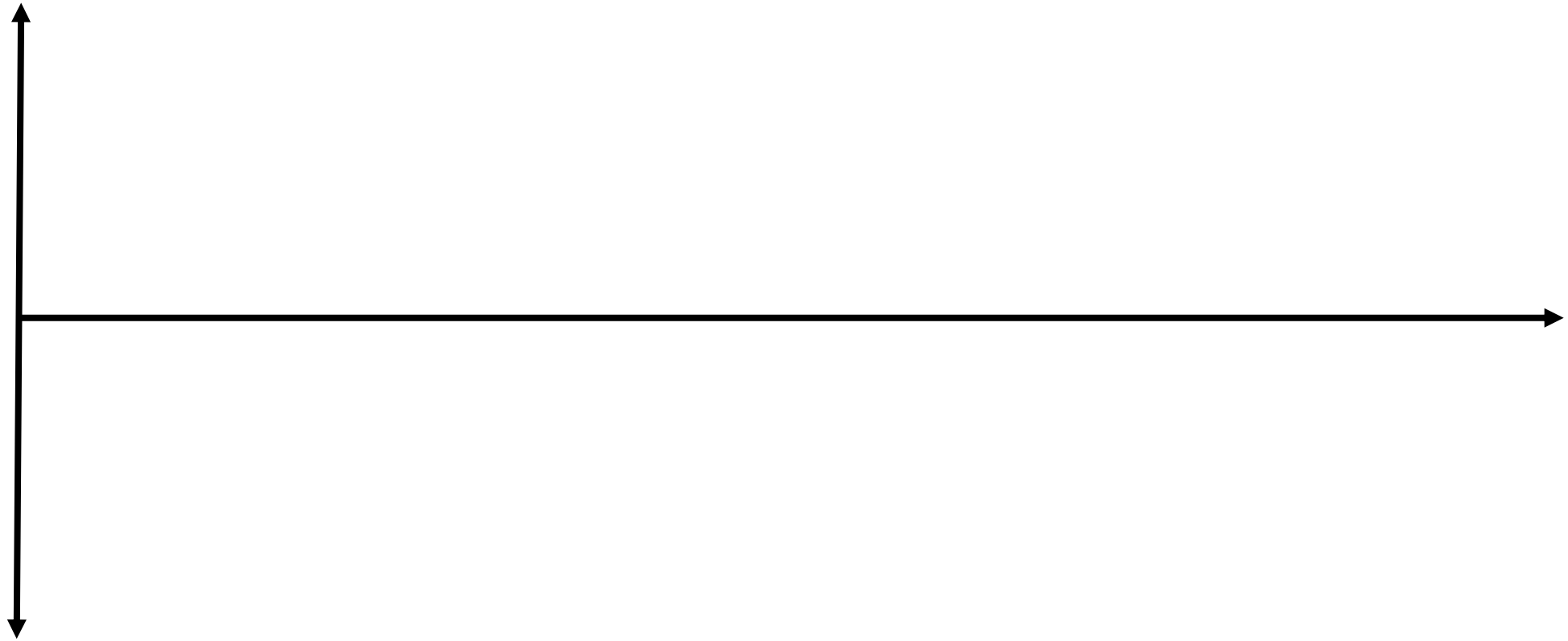
Der Digitale Ersthelfer im Einsatz

- Ein Kollege in der HR-Abteilung öffnet aus Versehen den Anhang einer „Bewerbung“. *Dateien.zip.exe* haben wohl keine Bewerbungsdateien ergeben, sondern eine schwarze Dosbox…
- Da eine Abteilungskollegin Digitale Ersthelferin ist, spricht er sie an
- Sie hört sich die Situation und den Ablauf an, lässt sich die E-Mail zeigen und wertet dies dann als möglichen Sicherheitsvorfall
- Sie zieht das Netzwerkkabel, beruhigt den Kollegen, bittet ihn, den PC ab sofort nicht mehr zu benutzen und zieht die internen IT-Experten hinzu
- Diese stellen fest, dass der Rechner tatsächlich kompromittiert ist und mit einer Schadfunktion ausgestattet ist, die versucht, im Ethernet übertragene Passwörter auszuspähen
- Der Vorfall wurde frühestmöglich gestoppt!



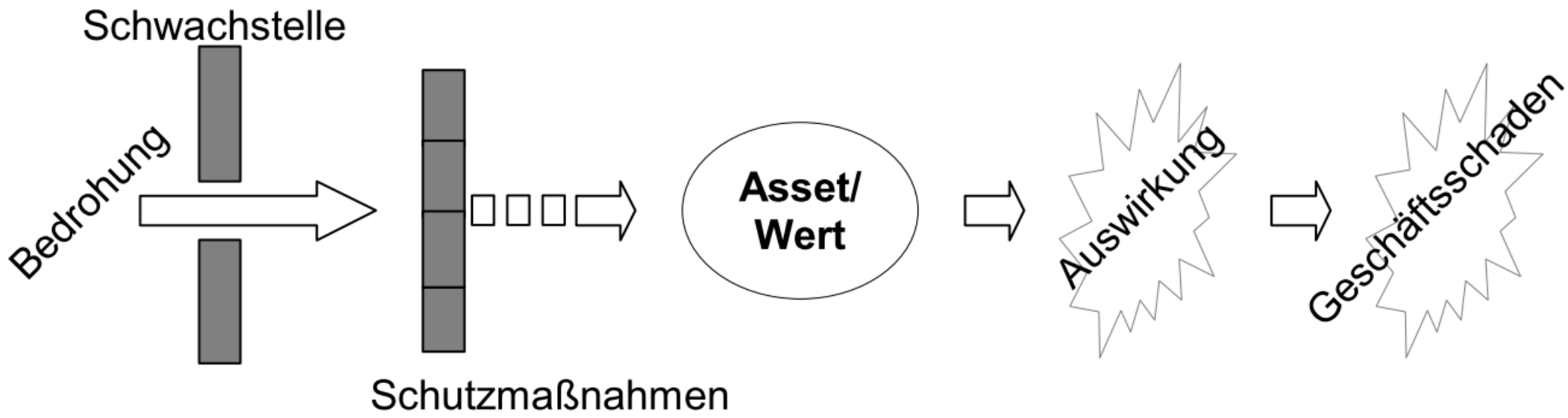
Vorstellung von und Arbeit mit Fallbeispielen

(Gefühlte) Kontrolle über einen Vorfall im Laufe der Zeit, kritische Punkte



Die gute Nachricht?

Interaktion von IT-Sicherheitselementen und Auswirkung auf Organisationsrisiken



Grundlagen: Kern des Problems

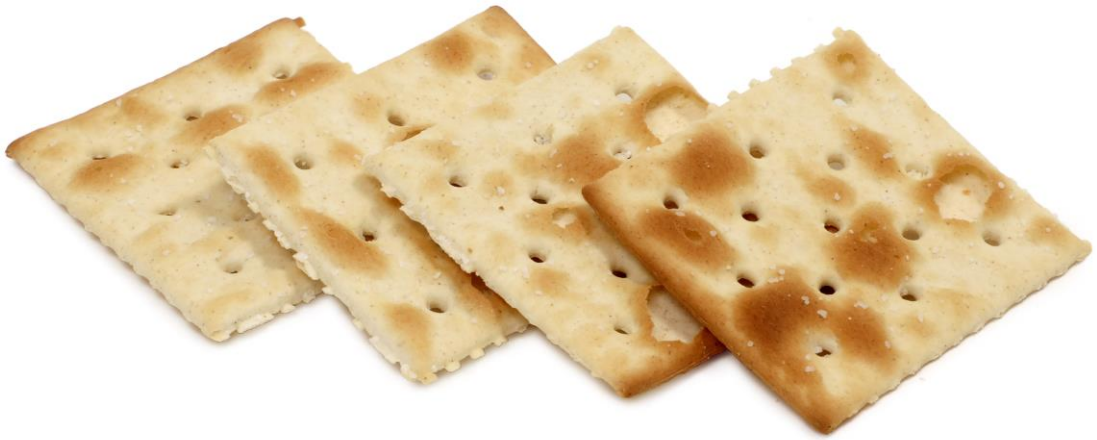
Tätergruppen / Tätermöglichkeiten und Tätermotivation

Hacker spähten Online-Banking Login-Daten aus. xijian/iStock.com

Dienstag, 03.01.2017, 15:37

Professionelle Hacker knacken fast alles, wie vor kurzem der Angriff

Quelle: focus.de



Hacker

Cracker

Grundlagen: Kern des Problems

Tätergruppen / Tätermöglichkeiten und Tätermotivation

„Ein Hacker ist jemand, der versucht einen Weg zu finden, wie man mit einer Kaffeemaschine Toast zubereiten kann.“

-- Wau Holland,
Mitgründer des
Chaos Computer Clubs

„ **Cracker** (vom englischen *crack* für „knacken“ oder „[ein]brechen“) umgehen oder brechen Zugriffsbarrieren von Computersystemen und Rechnernetzen.“

-- Wikipedia,
Cracker (Computersicherheit)

Hacker

Cracker

Grundlagen: Kern des Problems

Gibt es (noch) einen Unterschied zwischen „extern“ und „intern“?

- Viele Unternehmen denken noch immer: *„Wir werden von extern angegriffen, also lassen wir mal (nur) unsere externen IP-Adressen mit einem Penetrationstest checken“*
- Angreifer denken bereits seit langem: *„Hm, soll ich aufwändig nach einer 0-Day-Lücke in der externen Firewall suchen, oder schicke ich einfach ein paar gut gemachte E-Mails mit etwas Schadcode?“*
- Im Ergebnis sollte man bei vielen Organisationen davon ausgehen: **extern=intern**
- Durch Homeoffice hat sich dies verschärft

Grundlagen: Kern des Problems

Was, wenn einmal private Geräte betroffen sind?

- Sind Privatgeräte „Forensic Ready“?
- Sind Mitarbeiter damit einverstanden, dass jemand zu Ihnen nach Hause kommt und/oder ihre Geräte untersucht?
- Sind Mitarbeiter überhaupt erreichbar? Oder gerade draußen Rasen mähen… ;-)

Grundlagen: Kern des Problems

Tätergruppen / Tätermöglichkeiten und Tätermotivation

- Akteure lassen sich klassifizieren nach
  - Fähigkeit: Sicherheitsexperten, Exploit-Programmierer, Script- Kiddies
  - „Farbe“: **Hacker , Cracker**, White-, Grey-, Black-Hat
  - Motivation für Angreifer: Fun, Ansehen, wirtschaftliche, politische oder militärische Interessen
  - Organisation: Alleine, Gruppe, vernetzte Gruppe
  - Beziehung zum Opfer: Innentäter, Außentäter
- Täter rangieren dabei vom
  - „Spaßtäter“ über
  - „einfache“ Kriminelle und organisierte Kreise bis hin zu
  - staatlich geförderten oder aufgestellten Täterkreise: Spionage, Cyber-War
- Zielgerichtete vs. „Massenangriffe“

Grundlagen: Kern des Problems

„Bereinigung“ einer kompromittierten IT-Umgebung

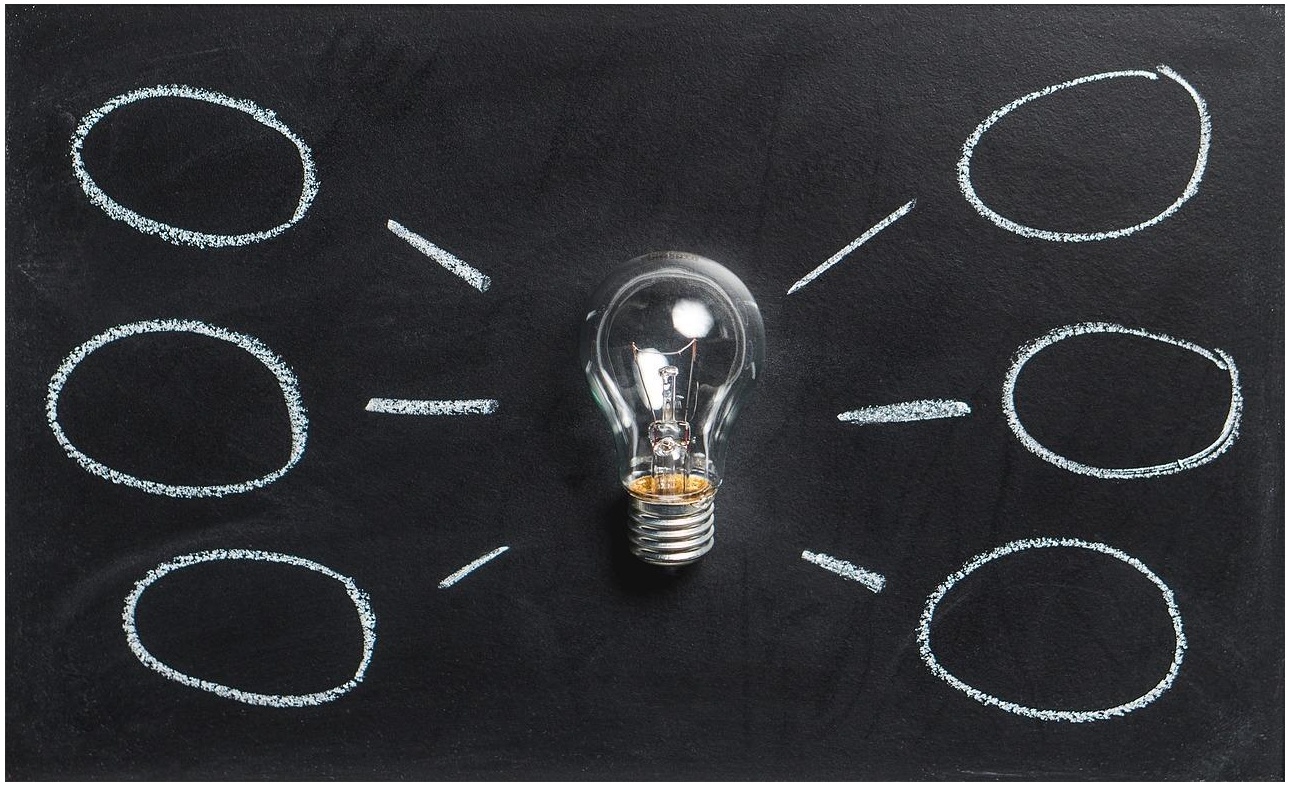
- Wann kann man sagen „Ich bin wieder sauber/schadcodefrei"?
- Kann man das überhaupt sagen?
- **In der Praxis: JEIN bis NEIN**

- Die wesentliche Frage lautet: Wie groß ist das Restrisiko?
- Leistungsspektrum der Experten: Abschätzen
- Ihre eigene Verantwortung: Entscheiden und verantworten

- Im Zweifel: Technik komplett neu beschaffen

Grundlagen: Kern des Problems

Was ist Forensic Readiness für Sie?



Grundlagen: Kern des Problems

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: Kern des Problems

Was ist IT-Forensik?
Klassische Vorstellung eines Forensikers:

Quelle linkes Bild: Ralf Roletschek, publiziert unter GFDL 1.2

Grundlagen: Kern des Problems

Was ist IT-Forensik?

„Forensik ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen kriminelle Handlungen systematisch untersucht werden. Der Begriff stammt vom lateinischen forensis „zum Forum, Markt(platz) gehörig“, da Gerichtsverfahren, Untersuchungen, Urteilsverkündungen sowie der Strafvollzug im antiken Rom öffentlich und meist auf dem Marktplatz durchgeführt wurden.“

- (Zitat: deutsche Wikipedia)

- Wortherkunft: Rechtssprechung
- Heutzutage: auch viele private Einsatzbereiche

Grundlagen: Kern des Problems

Was ist IT-Forensik?

Häufiger Fokus: wer hat was wann (warum) gemacht

Menschen <-> Daten

Grundlagen: Kern des Problems

Was ist IT-Forensik?

Totforensik (post mortem)

Live-Forensik

Netzwerkforensik

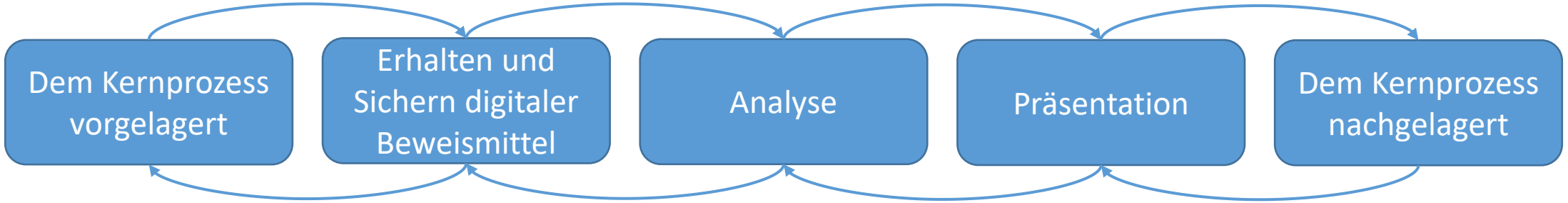
Sachverständigengutachten

eDiscovery

Sicherheitsvorfall

Datenabfluss

Compliance-Verstoß



Grundlagen: Kern des Problems

Exkurs: Locard‘sche Regel / Locard‘sches Prinzip

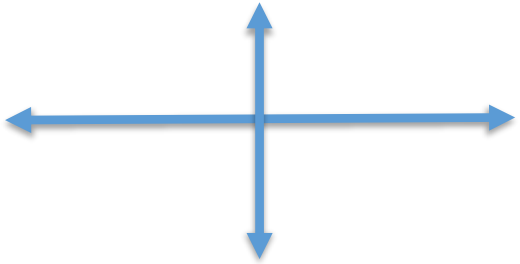
- Kontakt zwischen zwei Objekten (Täter, Opfer, Tatort, …) nicht möglich ohne wechselseitige Spuren
- Gilt in der Praxis auch in der IT:
  - Täter hinterlässt Logdatei-Einträge
  - Täter löscht Logdatei, hinterlässt aber gelöschte Datei im Dateisystem
  - Täter überschreibt Datei vorher, hinterlässt dadurch aber wieder Einträge in anderer Logdatei
  - …
- Wichtig: auch eigene Aktionen hinterlassen Spuren, oder „verwischen“ Einbruchsspuren!

Grundlagen: Kern des Problems

Herausforderungen aus Sicht des Geschäftsführers

Juristische Herausforderungen

Interne / taktische Herausforderungen



Finanzielle Herausforderungen

Technische Herausforderungen

Grundlagen: Kern des Problems

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: Kern des Problems

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: Kern des Problems

Ziele können sich ergänzen oder gegenseitig behindern

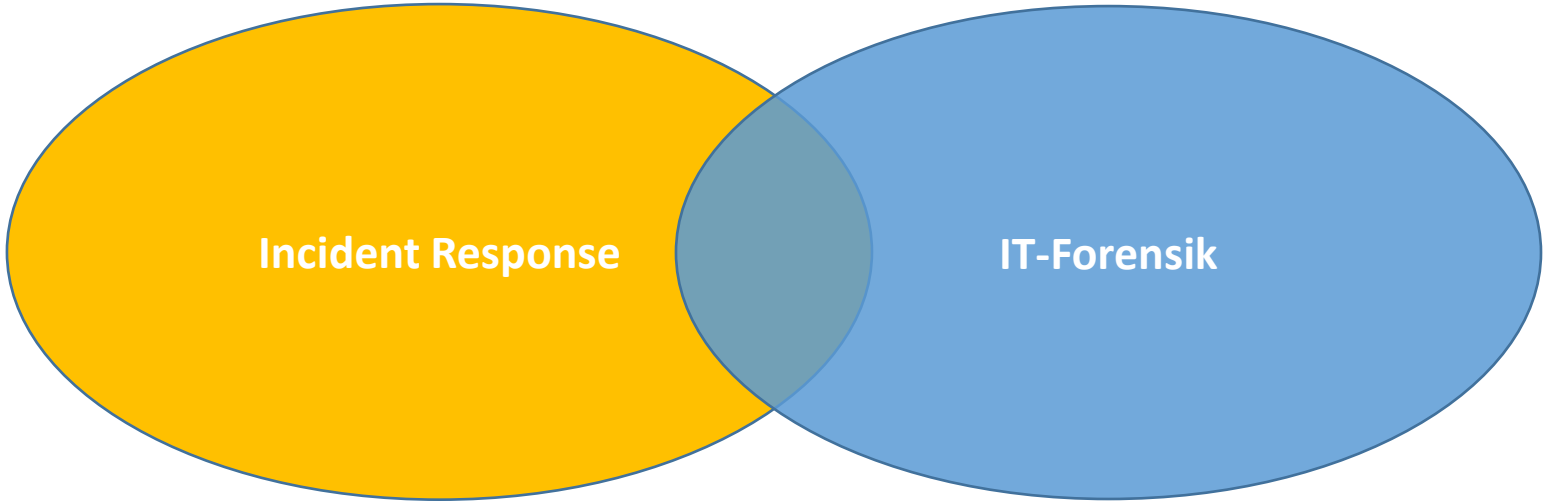
- Angriff stoppen oder laufen lassen?
- Zukünftige Angriffe verhindern?
- Täter finden?
- Hergang aufklären?
- Mitarbeiter einbeziehen oder auslassen?
- Ermittlung/Strafverfolgung einbeziehen?
- Priorisierung?
- Systeme abschalten oder laufen lassen?
- Offen oder verdeckt ermitteln?

Verantworten muss letztlich der Geschäftsführer (oder IT-Leiter)

Grundlagen: Kern des Problems

Schnittmenge und Abgrenzung

- Hauptunterschied: Zielsetzung



Grundlagen: Kern des Problems

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: Kern des Problems

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: Kern des Problems

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:

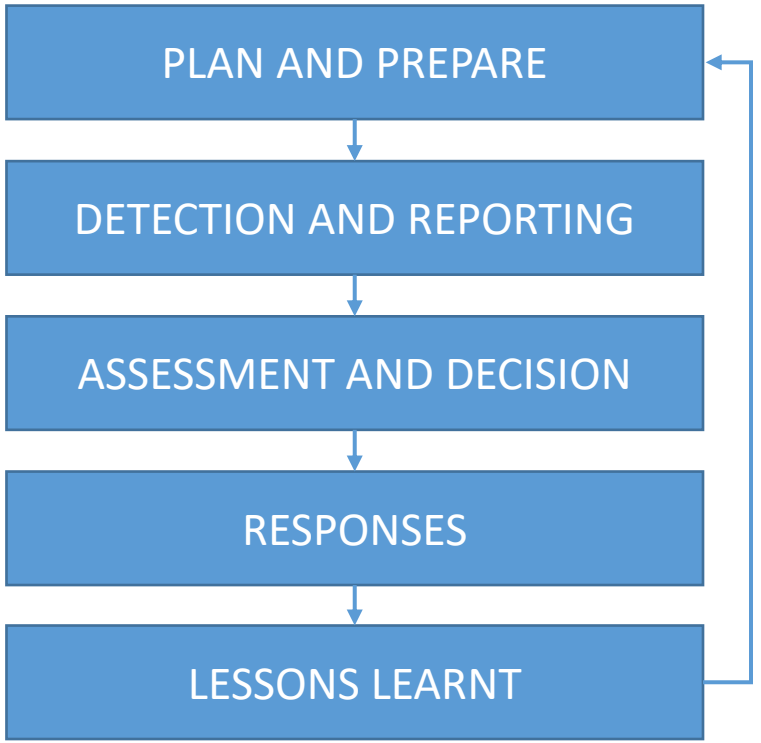
- ISO/IEC 27035-1
- ISO/IEC 27035-2
- BSI-Standard 100-4 (Notfallmanagement)
- BSI-Leitfaden IT-Forensik

Grundlagen: Kern des Problems

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: Kern des Problems

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: Kern des Problems

BSI-Standard 100-4

- Webkurs Notfallmanagement
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/Webkurs1004_node.html

Grundlagen: Kern des Problems

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: Kern des Problems (Corona?

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: Kern des Problems

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: Kern des Problems

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: Kern des Problems

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)

Grundlagen: 10-Punkte-Plan

Ein Vorschlag für bessere Forensic Readiness und damit besseres Incident Response

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

Grundlagen: 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

Grundlagen: 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?

Grundlagen: 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

Grundlagen: 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!

Grundlagen: 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

Grundlagen: 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?)
- …

Grundlagen: 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?)

Grundlagen: 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
- **Essentiell**: Backups so managen, dass diese auch vertrauenswürdig genug sind und nicht manipuliert/sabotiert werden können (z.B. geschützte Lagerung)

Grundlagen: 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
- …

Grundlagen: 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

Konzeptvorstellung „Digitaler Ersthelfer“

Die Rolle des „Digitalen Ersthelfers“

- Typisches Profil: IT-Laie, IT-erfahren oder sogar IT-Experte, aber kein Experte für IT-Forensik und Incident Response
- Wichtigste Tätigkeiten:
  - IT Incidents bemerken und erste Schritte einleiten
  - 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
  - Einfache Fälle auch selbst abschließend bearbeiten

Konzeptvorstellung „Digitaler Ersthelfer“

Achtung 1

- Der Digitale Ersthelfer ist nicht explizit gesetzlich verankert/geregelt
- Es handelt sich um ein neues/“freiwilliges“ Konzept

Konzeptvorstellung „Digitaler Ersthelfer“

Die Rolle des Digitalen Ersthelfers

- Digitaler Ersthelfer (DE):
  - Eine Person, die im Bereich „digital“ (IT) im Ernstfall „erste Hilfe“ leistet.
- Wer kommt als DE in Frage:
  - Sowohl IT-Laien als auch IT-Experten (z.B. Fachinformatiker, Informatiker oder langjährig Berufserfahrene)
  - Sie füllen diese Rolle dann mit ihrer jeweiligen Erfahrung und Qualifikation aus.
- Sorgt dafür, dass das was „menschenmöglich“ und zugleich notwendig ist, bis Experten für Incident Response und IT-Forensik (oder je nach Fall auch „normale“ IT-Experten) eintreffen und übernehmen, gemacht wird.

Konzeptvorstellung „Digitaler Ersthelfer“

Die Rolle des Digitalen Ersthelfers

- DE ist jemand, der eine Ersteinschätzung der Lage vornimmt und dann
  - unmittelbar Hilfe leistet (selbst direkt handeln), oder
  - mittelbar Hilfe Leistet (Hilfe von Dritten einholen)

- Ist Ansprechpartner für interne Kollegen: Fragen oder Hilfebedarf zu möglichen IT-Vorfällen
- Nimmt auch Erstmeldungen über mögliche IT-Vorfälle von Dritten entgegen
- Gibt jedoch keine Informationen nach außen!

Konzeptvorstellung „Digitaler Ersthelfer“

Tätigkeiten je nach IT-Qualifikation

- DE ist selbst IT-Experte:
  - Er kann (muss aber nicht) nach individueller Abwägung auch selbst einen Vorfall abschließend bearbeiten.
  - Gilt auch für kritische Vorfälle, wenn er entsprechend ausgebildet und erfahren ist.
- DE ist IT-Laie:
  - Er darf auf keinen Fall kritische Vorfälle allein oder abschließend bearbeiten.
  - Darf Vorfälle, die zweifellos erkennbar von niedriger Gewichtigkeit/Auswirkung sind abschließend bearbeiten.

Konzeptvorstellung „Digitaler Ersthelfer“

Aufgaben im Ernstfall

- Kommunikationssteuerung innerhalb des Teams, Erreichbarkeit seiner Person schaffen
- Beachten der eigenen Sicherheit (also nicht etwa potentiellen Schadcode auf dem eigenen System „austesten“)
- Holt in Abstimmung mit der Geschäftsführung Hilfe von externen Experten für IT-Forensik, Incident Response, juristische Beratung, PR, …
- Holt Hilfe von internen Experten für IT-Forensik, Incident Response, juristische Beratung, PR, …
- Informationssammlung in begrenztem Umfang (analog Meldekette medizinischer Notfall) und Vorfalldokumentation anhand eines vorab bereit gehaltenen Template

Konzeptvorstellung „Digitaler Ersthelfer“

Aufgaben im Ernstfall

- Weitergabe der Informationen und Dokumentation in Abstimmung mit der Geschäftsführung
- „Absicherung der Unfallstelle“
- „Rettung von Verunfallten“
- Kommunikation mit Dritten (z.B. Polizei, Presse) ausschließlich nach detaillierter Absprache mit und Freigabe durch die Geschäftsführung

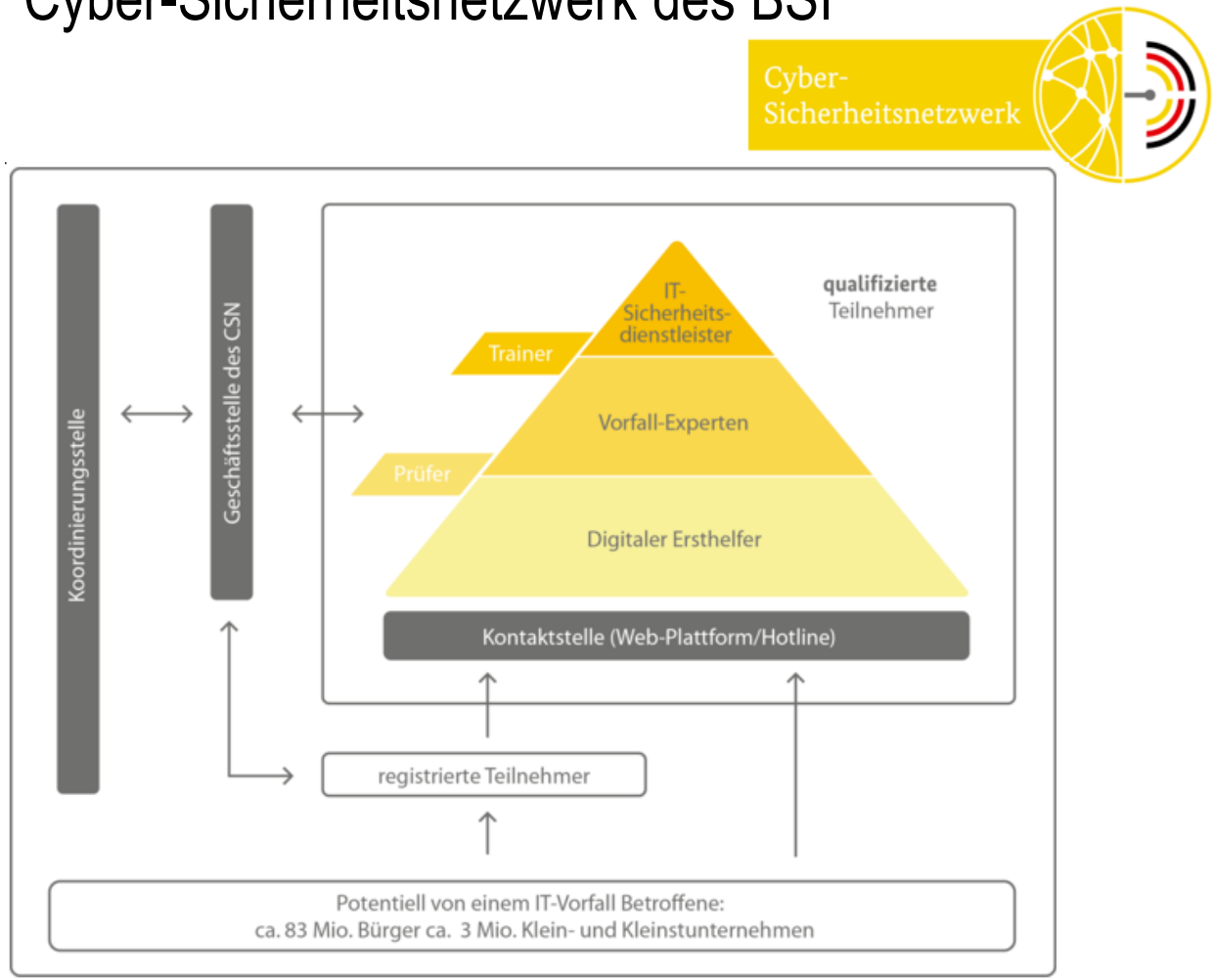
Konzeptvorstellung „Digitaler Ersthelfer“

Schlüsselkompetenzen eines Digitalen Ersthelfers

- Geeignet eskalieren
- Knapp und präzise Dokumentieren
- Strukturieren und Priorisieren
- Risiken managen
- Hilfe holen
- Offensichtliche Dinge bemerken
- Ruhe bewahren
- Stressfestigkeit

Konzeptvorstellung „Digitaler Ersthelfer“

Cyber-Sicherheitsnetzwerk des BSI



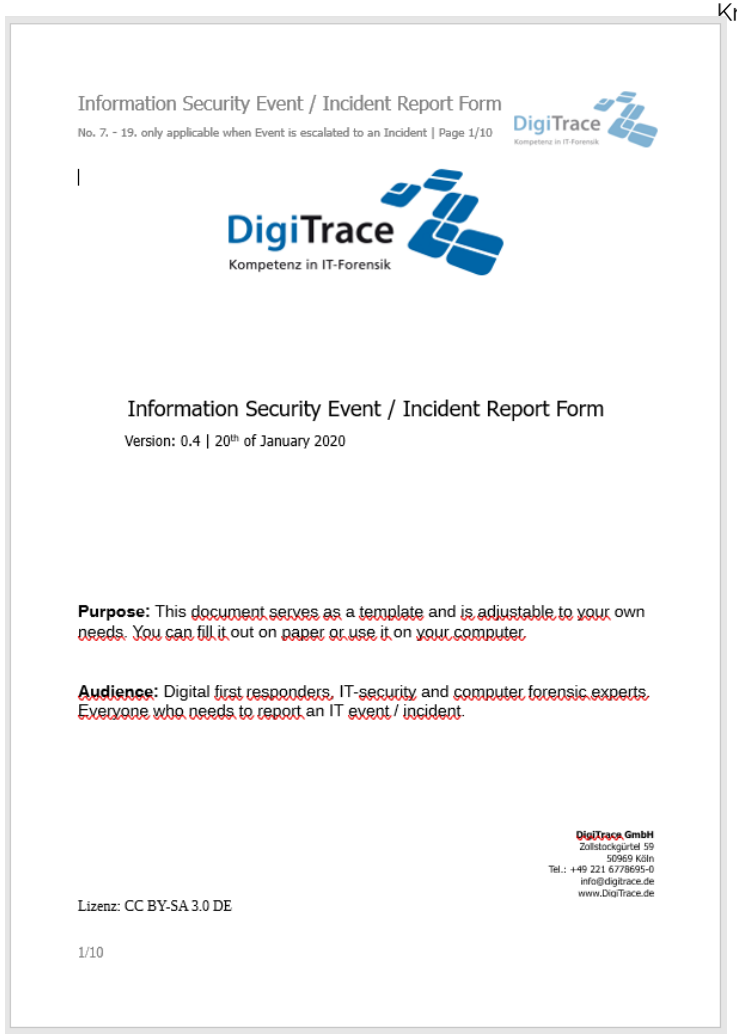
Quelle: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/cyber-sicherheitsnetzwerk_node.html

IT-Notfallkarte

Konzeptvorstellung „Digitaler Ersthelfer“

Sinnvolles „Werkzeug“: Erfassungsschablone (strukturierte Erfassung)

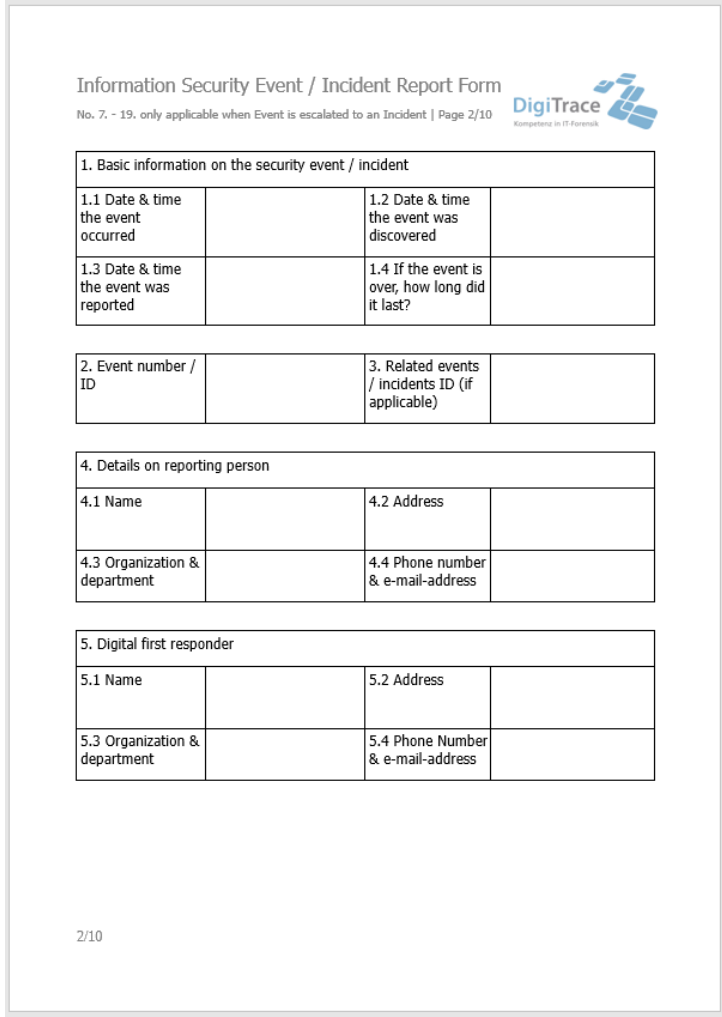
- Schablone zum Melden, Erfassen und Managen von Ereignissen
- Mindeststandard!
- Es gibt nicht „die eine“ Schablone
- Wichtigster Mehrwert: bringt Struktur und zeigt auf, was typischer Informationsbedarf ist



Konzeptvorstellung „Digitaler Ersthelfer“

Sinnvolles „Werkzeug“: Erfassungsschablone (strukturierte Erfassung)

- Letztlich dreht es sich um die **W-Fragen**, um
- **Schadenspotentiale** (was kann passieren) und damit um eine Hilfe, um
- **Maßnahmen sinnvoll auszuwählen und umzusetzen**
- Basis: von DigiTrace unter CC-BY-SA zur Verfügung gestellt



Information Security Event / Incident Report Form

No. 7. - 19. only applicable when Event is escalated to an Incident | Page 2/10

1. Basic information on the security event / incident			
1.1 Date & time the event occurred		1.2 Date & time the event was discovered	
1.3 Date & time the event was reported		1.4 If the event is over, how long did it last?	

2. Event number / ID		3. Related events / incidents ID (if applicable)	

4. Details on reporting person			
4.1 Name		4.2 Address	
4.3 Organization & department		4.4 Phone number & e-mail-address	

5. Digital first responder			
5.1 Name		5.2 Address	
5.3 Organization & department		5.4 Phone Number & e-mail-address	

2/10

Exkurs: juristische Aspekte

Was berechtigt / verpflichtet eine „normale Person“ (ohne Vertrag o.Ä.)?

- Personen, die nicht vertraglich zur digitalen Ersthelferschaft verpflichtet sind, trifft grundsätzlich auch keine Unterstützungspflicht (außer in Fällen von § 323c StGB)
- Die Motivation zur Hilfe erfolgt damit zumeist „freiwillig“, aus gutem Herzen, aus wie auch immer gearteter Verbundenheit ;-).
- Dieses lässt sich prinzipiell als „(echte) Geschäftsführung ohne Auftrag“ ansehen, weil diese Person dann für die Organisation ein „Geschäft“ besorgt, für das eigentlich die Organisation selber zuständig ist.
- Durch die Hilfe entsteht jedoch ein gesetzliches Schuldverhältnis mit „quasivertraglichen Ansprüchen“
- Er muss das „Geschäft“ jedoch so führen, wie es dem vermeintlichen Interesse der Organisation entsprechen würde
- Da der (selbstlose) digitale Ersthelfer zur Abwendung einer drohenden / dringenden Gefahr tätig wird, haftet er **nur für Vorsatz und grobe Fahrlässigkeit** – was sich wiederum nach den einzuhaltenden Sorgfaltspflichten bemisst…
- Und bei all dem sollte man auch niemals den „Gesetzesdschungel“ außer acht lassen…

Exkurs: juristische Aspekte

Pflicht zum Helfen – Strafbarkeit nach § 323 c StGB - Einleitung

- Bei § 323 c StGB wird bestraft, wer in einer Notsituation keine Hilfe (echtes Unterlassungsdelikt) leistet, obwohl er (aus welchen Gründen auch immer) dazu verpflichtet wäre – folgende Situationen sind denkbar:
  - Unglücksfall: Plötzlich eintretendes Ereignis, das erhebliche Gefahren für Personen oder bedeutende Sachwerte mit sich bringt oder zu bringen droht
  - Gemeine Gefahr: Zustand, bei dem die Möglichkeit eines erheblichen Schadens an Menschen oder bedeutenden Sachwerten für unbestimmt viele Personen nahe liegt (z.B.: Brand, Naturkatastrophen).
  - Gemeine Not: Eine die Allgemeinheit betreffende Notlage (z.B.: größere Hindernisse auf Fahrbahn).

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

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“

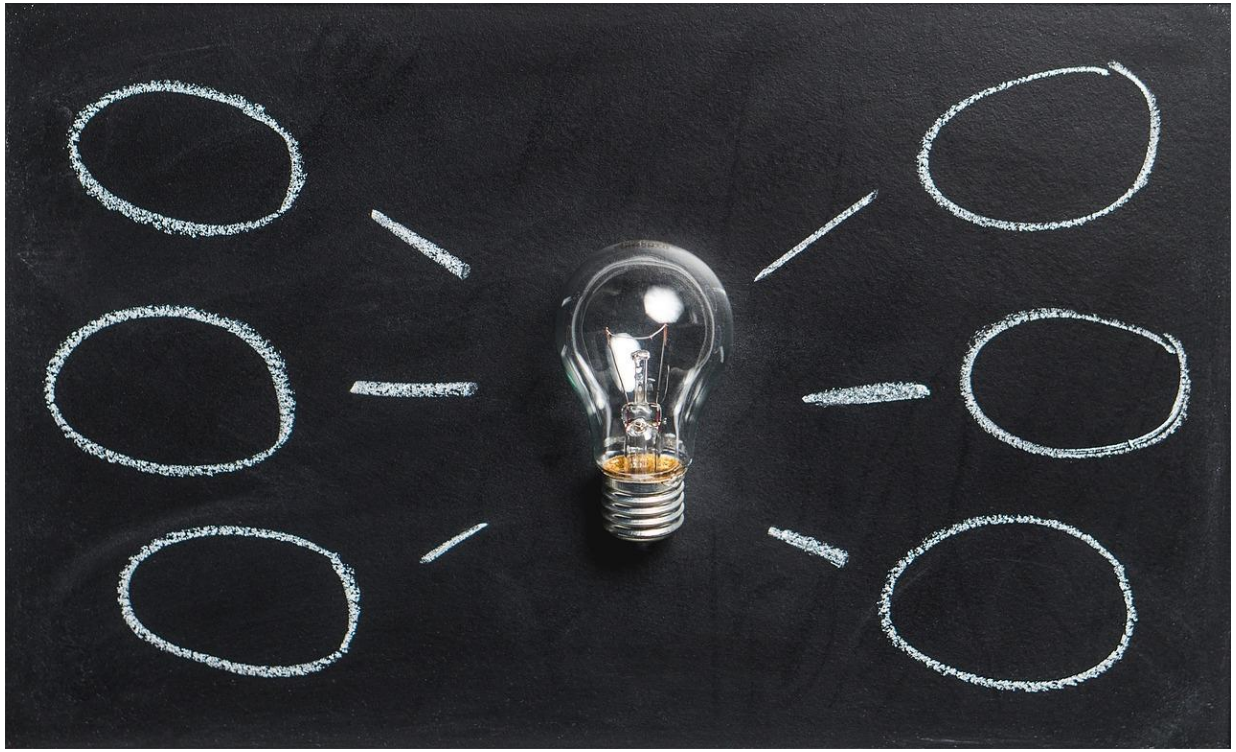
Rechtliche Einschränkungen

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 und Lösungen

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 und Lösungen

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 und Lösungen

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.

Typische Fehler und Lösungen

Beispiel „Emotet“: Situation „zuhause“ vs. im Organisationsumfeld

- Zuhause/Privat
  - Vermutlich nur ein PC/Laptop oder zumindest wenige Geräte
  - Eventuell eine gangbare Option:
    - PC „neu aufsetzen“
    - Passwörter ändern
    - Urlaubsbilder etc. aus Backup wieder einspielen
- Unternehmen/Organisationen
  - Viel IT (heterogen/komplex)
  - Vermutlich/oft notwendig: Shutdown (Infektion breitet sich oft noch aktiv aus)
  - Passwörter ändern
  - „Vertrauenswürdigen Kern“ schaffen (z.B. komplett neue Geräte für die IT-Abteilung)
  - Wirksam getrennte Netzwerkzonen bilden
    - „sauber“
    - „unklar“
    - IT-Admin
    - …

Typische Fehler und Lösungen

Allgemein: Teamwork

- Strukturiertes Team mit Hauptansprechpartner aufbauen
- Interdispziplinär:
  - IT-Experten (Administratoren)
  - Incident-Response-Experten
  - …
- Auskünfte/Feststellungen (konstruktiv) kritisch hinterfragen
- Zentrale Dokumentation (eine Möglichkeit: Wiki)
- Wichtiger Erfolgsfaktor: angemessene Beteiligung der Entscheider

Typische Fehler und Lösungen

Allgemein: Bestandsaufnahme und Priorisierung

- Wurden eventuell auch Daten abgegriffen (Leaking, Doxing)?
- Wurden eventuell Daten „subtil“ manipuliert?
- Notbetrieb planen anhand der Abhängigkeit der einzelnen Geschäftsprozesse von IT-Ressourcen und IT-Prozessen
- Dies ermöglicht eine Auswahl und Priorisierung von Maßnahmen (z.B. Not- und Bereinigungsmaßnahmen)

Fazit

Rückblick: bewältigen Organisationen IT-Vorfälle zuverlässig, schnell und sicher?

- Viel wertvolle Zeit geht zwischen Vorfall und Entdeckung verloren
- Zu oft werden falsche Prioritäten gesetzt, Spuren vorschnell „verwischt“ oder befallene Systeme zu lang weiter verwendet
- Ein systematisches Problem liegt im häufigen „Blindflug“: Systeme erstellen zwar Ereignisprotokolle, diese werden aber nicht aggregiert, ausgewertet und überwacht
- Hinzu kommt vermeidbarer Stress, wenn ein Vorfall bemerkt wird
- Um so wichtiger ist es, Menschen (uns!) in die Lage zu versetzen, mit einfachen „Handgriffen“ IT-Auffälligkeiten besser erkennen und schnell Hilfe holen zu können

Diskussionsrunde und Ausblick

Zusammenfassende Einschätzung

- Erfahrungen aus der IT-Forensik und aus Penetrationstests
  - Standards/Prozesse/Rahmenwerke sind notwendig aber nicht hinreichend
  - Erst durch (zusätzliche) konkrete Tests kann hinreichende IT-Sicherheit entstehen
- CERT, SIEM, SOC, etc. und doch falsch reagiert – Weltenbruch und Komplexität als Problem
  - KMU: wir haben keine Ressourcen um diesen Windows 2003 Server abzulösen
  - Konzern: „Hm, diesen Windows 2003 Server haben wir unter unseren 5.000 anderen Serversystememem wohl übersehen“
- Werkzeugkoffer für Reaktionsmöglichkeiten
  - Zusätzliches „Werkzeug“: Digitaler Ersthelfer
- Cyber Security in die einzelnen Business-Abteilungen tragen
  - Digitaler Ersthelfer

Fazit/Rückblick und Ausblick

Die „Guten“ werden noch besser, aber was ist mit den „Schlechten“?

- Aus meiner Sicht:
  - Konkrete Gefahr einer noch immer bestehenden „Spreizung“ (vielleicht ohnehin schon immer?) bei Herstellern/Betreibern/Anwendern in Bezug auf Kompetenz/Erfahrung/Professionalität/Ressourcen/Sorgfalt
  - Daran lohnt es sich zu arbeiten! ☺

Diskussionsrunde und Ausblick

Gibt es den „Readiness-Trick“?

Ja! Reden Sie miteinander. Seien Sie als Ansprechpartner wirklich erreichbar, auch für Externe. Gehen Sie den Dingen auf den Grund.

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, Vorstandsmitglied AKEUR e.V., Vorstandsmitglied des Bundesverbandes für den Schutz Kritischer Infrastrukturen (BSKI) e.V.

Geschäftsführer und Gründer der DigiTrace GmbH

Teamgröße am Standort Köln: 10 IT-Experten

Kunden von KMU bis Konzerne + Behörden, **insb. auch im Bereich KRITIS**

- 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

DigiTrace: Gründungsmitglied des BSKI

BSKI

- Der Bundesverband für den Schutz Kritischer Infrastruktur (Abk.: BSKI) e.V. wurde im Juni 2018 als Vertretung von Interessen aus dem Bereich Kritischer Infrastrukturen gegründet.
- Der BSKI ist die zentrale Anlaufstelle für Entscheider aus Kritischen Infrastrukturen, um ganzheitliche Schutzkonzepte zu etablieren.
- Der BSKI e.V. ist eine Interessenvereinigung, die die Interessen aller KRITIS-Einrichtungen und Betroffene nach außen hin vertritt und seinen Mitgliedern auch konkrete Hilfe durch Informationen und Serviceangebote zur Verfügung stellt.
- www.bski.de

Kurzvorstellung DigiTrace

DigiTrace
Kompetenz in IT-Forensik

Womit unterstützen wir?

ZAHLEN UND FAKTEN

Gegründet 2011 von Martin Wundram und Alexander Sigel, die beide Geschäftsführer und alleinige Gesellschafter sind (eigenkapitalfinanziert).

Seit 2013 Ausbildungsbetrieb. Teamgröße: 8 IT-Experten. Vom Standort Köln aus in die Welt: national und international tätig. Alle Mitarbeiter sind einschlägig qualifiziert und z.T. bereits seit Ausbildung/Studium bei DigiTrace.

Unser Team hat hunderte Projekte realisiert, hunderte Gutachten geschrieben, dutzende Vorträge sowie Schulungen durchgeführt.

beweisbar authentisch – unabhängig – sachverständig

IT-FORENSIK

Sachverständige Aufklärung mit Leidenschaft und Methodik: Sie haben Fragen zu auffälligen Sachverhalten, bei denen Datenspuren zur Erhellung beitragen können?
ind beurteilen
d von Datenquellen
er und beantworten

INCIDENT RESPONSE

Gekonnt reagieren im IT-Ernstfall: Bei IT-Sicherheitsvorfällen oder Notfällen unterstützen wir Sie kurzfristig. Wir beurteilen IT-Schäden und helfen Ihnen, diese zu minimieren, Notfallmaßnahmen umzusetzen, so wieder in den Normalbetrieb zu gelangen und Ihre Systeme gegen Angriffe zu härten. I
und erkennen und managen Ihre Risiken.

IT-SICHERHEIT | PENTESTS

Wir fordern Sie heraus – als Sparringspartner: Egal ob 1 oder 4.000 Server – unsere Penetrationstester beherrschen verschiedenste Tätersimulationen, Black- wie White-Box-Vorgehen für Angriffe auf externe wie interne IT-Systeme und -Netze sowie auf Webanwendungen. Techniker wie Manager verstehen die in unseren Berichten aufgezeigten Schwachstellen und wie sie geschlossen werden können.

eDISCOVERY

Heiße Spuren treffsicher finden und beurteilen: Sie suchen in großen Datenmengen nach „der Nadel im digitalen Heuhaufen"? Mit Know-How, Methodik nach EDRM und geeigneten Werkzeugen und Systemen stellen wir beweisrelevante Daten sicher und bereiten diese verdichtend auf. Sie reviewen auf unserer Analyseplattform oder betrauen uns auch mit der inhaltlichen Durchsicht.

IT-BERATUNG

Mit Sachverstand passende Lösungen erarbeiten: Profitieren Sie vo
in IT-Forensik und IT-Sicherheit, um Ihr Problem zu lösen. Uns treibt de
– Organisation – Technik, denn Investition in nur mehr Technik wird Sie
Fragen Sie z.B. nach Schutzbedarfsanalysen und -konzepten, Angriffss

SCHULUNGEN

Know-How teilen – mit Ihnen: Sie lernen mit uns für Sie relevante Konzepte und ihre praktische Anwendung in der IT. Unsere Trainer schöpfen ihr Wissen authentisch aus eigener Projekterfahrung, insbesondere in IT-Forensik und IT-Sicherheit, und

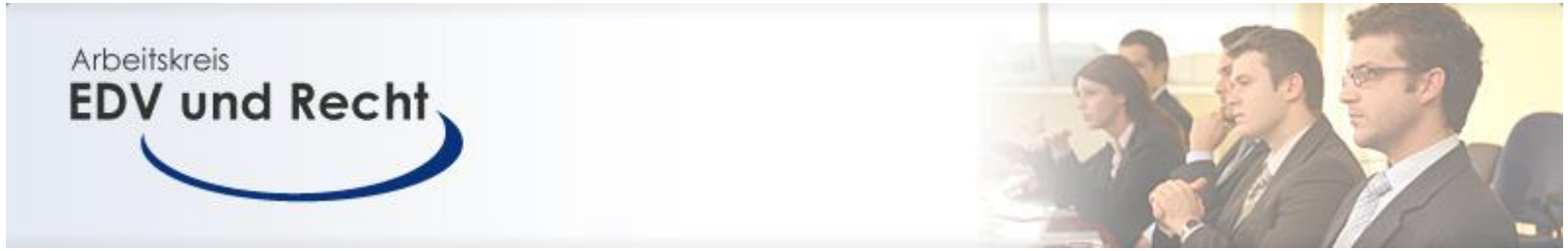
VORTRÄGE

Von Keynote bis Fachvortrag – wir berichten aus erster Hand: In unseren Vorträgen (Präsenz und online) zu IT-Forensik und IT-Sicherheit vermitteln wir seriös und verständlich den ernsthaften Kern des Themas. Sie erfahren aktuelle Entwicklungen und Einschätzungen aus dem Blickwinkel von Spezialisten, erhalten Denkanstöße und Handlungsempfehlungen oder erleben besondere Live-Hacks.

DigiTrace: Martin Wundram Vorstandsmitglied im AKEUR

Arbeitskreis EDV und Recht e.V.

- Der "Arbeitskreis EDV und Recht" bietet an der Schnittstelle zwischen Recht und elektronischer Datenverarbeitung ein Forum für Austausch und Zusammenarbeit seit 1998.
- Das Ziel ist die Verbesserung der Verständigung zwischen Juristen und IT-Professionals.
- Bei den Veranstaltungen des "Arbeitskreises EDV und Recht" werden daher aktuelle Themen aus dem Bereich der Informationstechnologie stets aus juristischer und technischer Sicht beleuchtet: Kompetent und fachspezifisch, nach dem Motto "Eintauchen in die Welt des anderen", und auf einer Ebene, die von allen Teilnehmern verstanden wird. Unsere Ziel ist intensive Diskussion und reger Austausch zwischen den Vertretern der angesprochenen Fachgebiete auch über die Veranstaltungen hinaus.
- www.akeur.de



DigiTrace: Sponsor des Kölner Kreis

Kölner Kreis

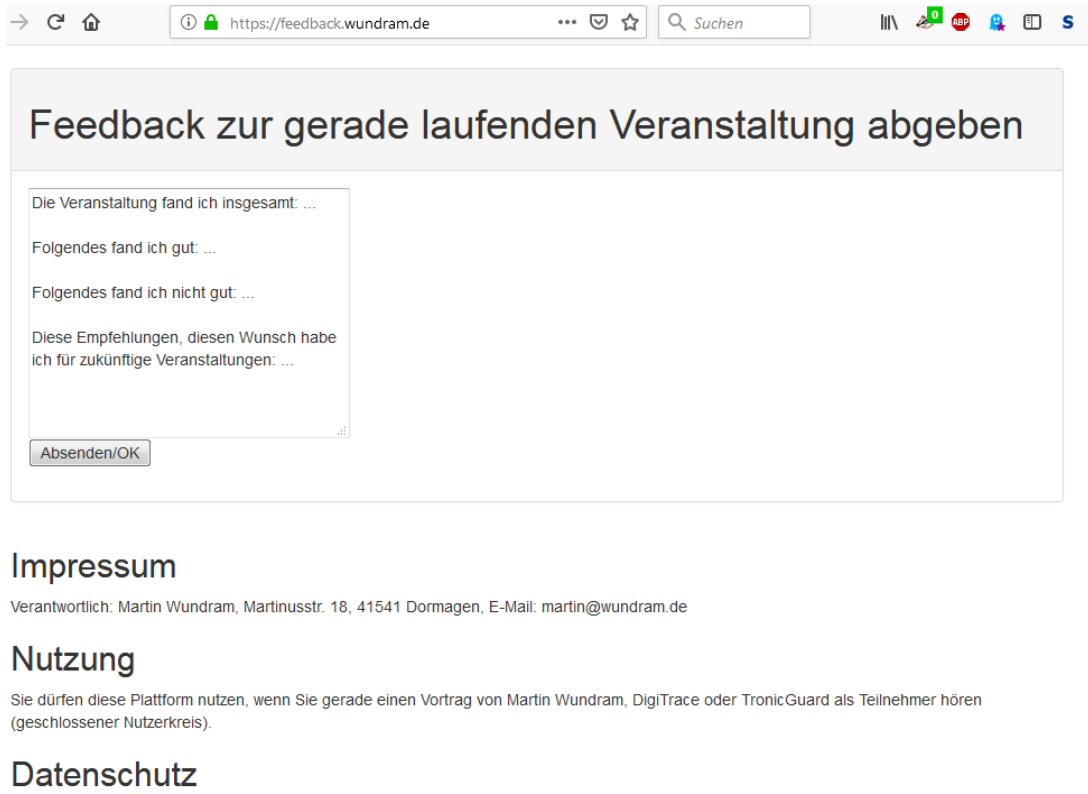
- Der „Kölner Kreis“ ist seit 2012 der Austauschtreff in Köln zu Themen rund um IT-Sicherheit und IT-Forensik. Wir treffen uns in lockerer Atmosphäre und zu besonderen Anlässen.
- Verschiedene Referenten halten Vorträge oder führen Workshops mit den Teilnehmern durch. Auch Diskussionsrunden bieten in angeregten Gespräche Gelegenheit zum Erfahrungsaustausch.
- Die Teilnahme steht Allen offen und ist kostenfrei.

www.kölnerkreis.de | www.koelnerkreis.de

Diskussionsrunde und Ausblick

FOLIEN-DOWNLOAD ab morgen

- Anonymes Feedback-System und Folien-Download: https://feedback.wundram.de



Diskussionsrunde und Ausblick

Fragen

&

Antworten

Gerne auch im Nachgang an

Martin.wundram@bski.de