

Informationssicherheit und IT-Forensik



4-01 – Incident Response

Lernziel dieser Einheit

- Wesentliche Aspekte und Herausforderungen bei Erkennung von und Reaktion auf IT-Vorfälle kennen
- Verstehen, dass und warum sich verschiedene Ziele gegenseitig behindern können
- Wesentliche Normen kennen und bei Bedarf heranziehen können
- Die „10 Goldenen Regeln des Digitalen Ersthelfers“ kennen

- „Better safe than sorry“ – Ein Fehlalarm ist besser als ein übersehener Sicherheitsvorfall

Trojanisierte Android-App verrät Raubkopierer

- 02.04.2011, HotHardware
- Eine manipulierte Version der Original-App “Walk and Text” (2,10 USD) mit einer gefährlichen Funktion.
- Folgende Nachricht wird an ALLE Einträge im Adressbuch per SMS versendet: ***"Hey, just downlaoded [sic] a pirated app off the internet, Walk and Text for Android. Im stupid and cheap, it costed [sic] only 1 buck. Don't steal like I did!"***
- Quelle: <http://hothardware.com/News/Shame-on-You-Pirated-Android-App-Really-Shameware/>

Googles Herzstück attackiert

- 19.04.2010, New York Times
- Ende 2009 gelang es Tätern mit möglicherweise chinesischem Background in das zentrale Authentifizierungssystem Gaia von Google einzudringen.
- Die chinesische Regierung bestreitet eine Verwicklung.
- Gaia wird für die Single-Sign-On-Anmeldung bei Google-Anwendungen für Millionen von Anwendern verwendet (z.B. Google Mail).
- Angriff begann mit einer Instant Message an einen Google-Mitarbeiter in China, welcher den darin enthaltenen Website-Link anklickte und darüber seinen PC infizierte.
- Durch den infizierten PC konnten die Täter auf andere Entwickler-PC und darüber auf ein Software-Repository zugreifen.
- Quelle: <http://www.nytimes.com/2010/04/20/technology/20google.html>

Geschichte: aus Fehlern anderer lernen

„Nichts sehen, nichts hören, nichts sagen“

Cryptotrojaner in einem medizinischen Großlabor

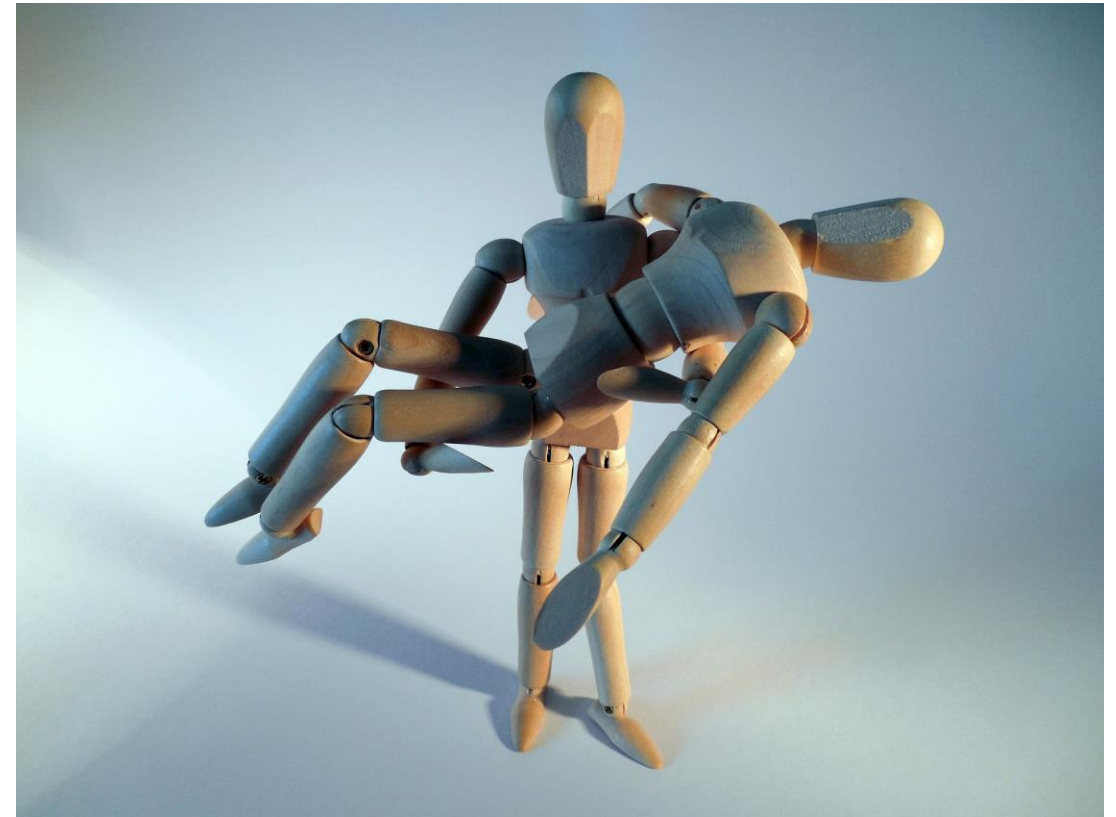
- Zunächst extreme Gefahr, weil Patientendaten (tausende einzelne Dateien) verschlüsselt sind. Funktionstüchtigkeit unklar.
- Selbstanalyse der eigenen IT: Backup funktionsfähig und vollständig.
- Analyse der IT-Forensiker: Standardschadsoftware einfacher Machart, kein zielgerichteter Angriff, vermutlich kein Folgerisiko. Täter können nicht gefunden werden.

Vorsätzliches Mitarbeiterfehlverhalten in Konzern

- Ein Mitarbeiter plant Wechsel in die Selbständigkeit und bereitet sich selbst ein „Abschiedsgeschenk“ vor:
 - Kopie von Bauplänen, Handbüchern, Schriftstücken auf (s)einen USB-Stick spätabends von dem PC eines Kollegen, aber mit seinem Domänen-Benutzerkonto
- **Gemeinsame Leistung von interner IT, Compliance und externem IT-Forensiker:**
 - SIEM (Systemüberwachung) hat auffällige Aktionen gemeldet (an IT)
 - IT hat Compliance eingeschaltet
 - Verdacht hat sich erhärtet, Compliance hat als First Responder direkt eine forensische Kopie des PCs erzeugt
 - Rahmenvertrag mit einem IT-Forensiker besteht -> unmittelbare Einzelbeauftragung möglich
 - Upload des PC-Abbilds in eRoom des IT-Forensikers
 - verzögerungsfreie Untersuchung und Bestätigung des Anfangsverdachts

Der Digitale Ersthelfer im Einsatz

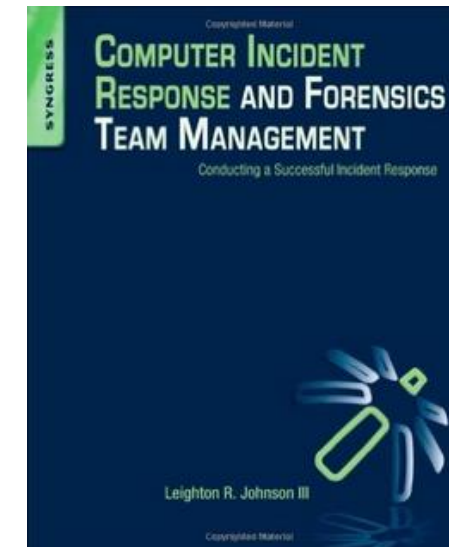
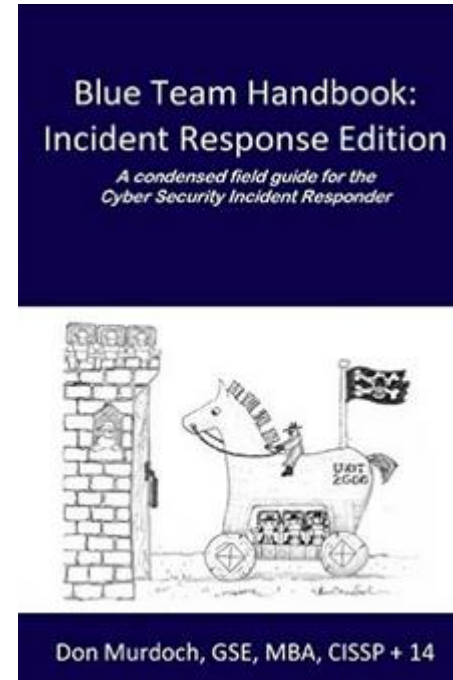
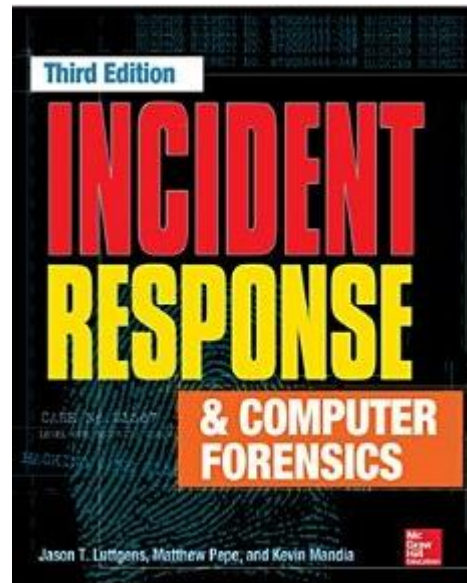
- Ein Kollege in der HR-Abteilung öffnet aus Versehen den Anhang einer „Bewerbung“. *Dateien.zip.exe* haben wohl keine Bewerbungsdateien ergeben, sondern eine schwarze Dosbox...
- Da eine Abteilungskollegin Digitale Ersthelferin ist, spricht er sie an
- Sie hört sich die Situation und den Ablauf an, lässt sich die E-Mail zeigen und wertet dies dann als möglichen Sicherheitsvorfall
- Sie zieht das Netzkabel, 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!



Zwischenfazit

- 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.
- Es reicht heute nicht mehr, „befallene“ PC einfach nur zu „säubern“

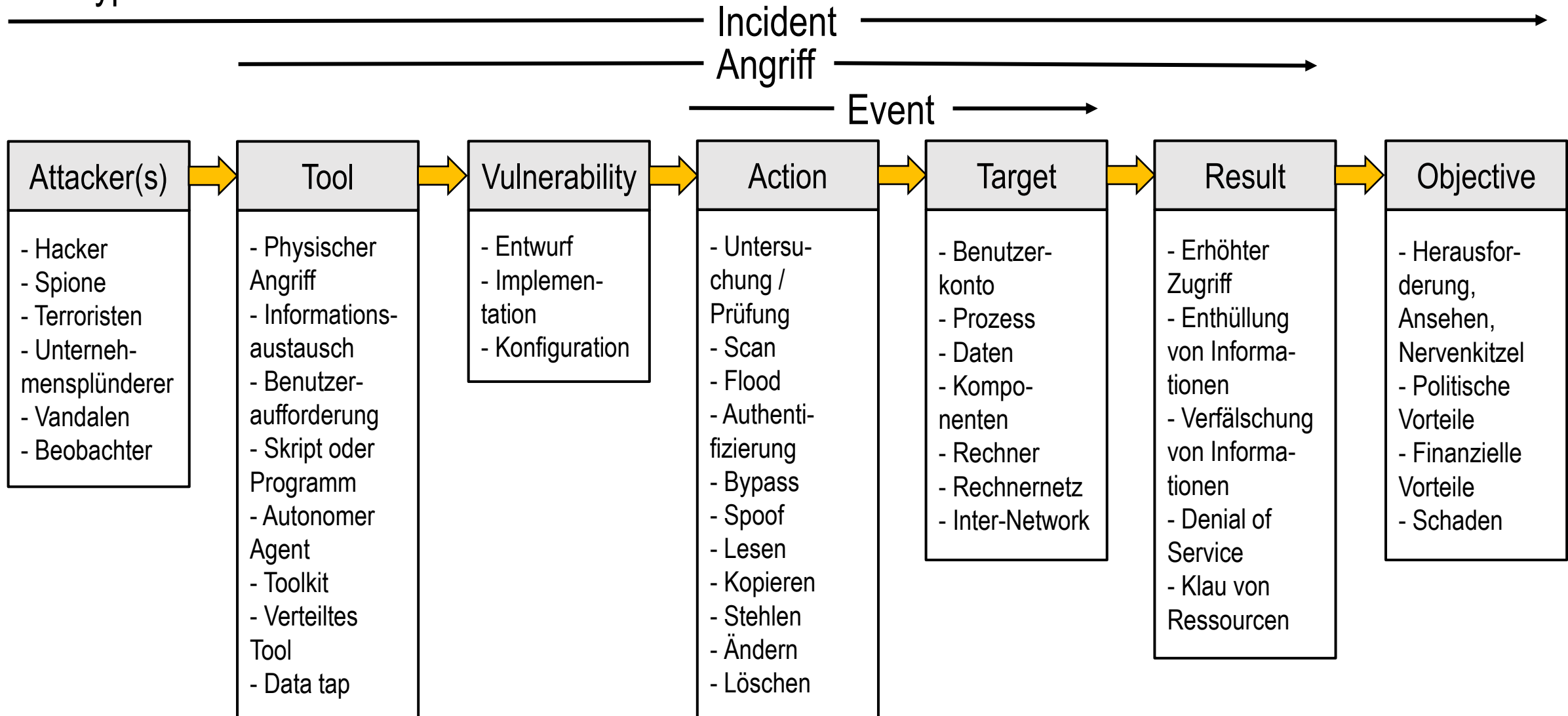
Geeignete Literatur



Mögliche Definitionen

- **Ereignis (Event):** 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
- Weitere Begriffe als „Eskalationsstufen“: Notfall, Krise, Disaster
- Störfall oder Sicherheitsvorfall?
- Festplatte geht durch Verschleiß kaputt vs. Innentäter sabotiert IT, tritt gegen Server

Typische Elemente eines IT-Incidents



Innentäter

- Beispiele:
 - Ein Mitarbeiter ist äußerst unzufrieden und richtet seinen Frust gegen das Unternehmen: Er löscht Daten oder tritt gegen Server
 - Ein Mitarbeiter möchte seinem neuen Arbeitgeber ein „Willkommensgeschenk“ bereiten und kopiert dazu allerlei vertrauliche Daten auf einen USB-Stick/Cloud/Mobiltelefon/...
- Was man als Ersthelfer tun kann:
 - Besonders vorsichtig sein, mit wem man kommuniziert
 - Auf keinen Fall einer „Hexenjagd“ verfallen
 - Weder zu früh einen Innentäter kategorisch ausschließen noch zu früh externe Täter ausschließen
 - Besonderen Fokus auf Wahrnehmungs- und Gesprächsprotokoll legen

Unauthorisierter Zugriff auf interne Daten

- Beispiele:
 - Unverschlüsselter Datenträger mit (vertraulichen) Daten verloren, etwa ein Mobiltelefon
 - Ein interner Dienst war über das Internet erreichbar (etwa File- oder Web-Server ohne Passwortschutz)
- Was man als Ersthelfer tun kann:
 - Prüfen, ob verlorene Geräte aus der Ferne gelöscht/gesperrt werden können
 - Erwägen, das betroffene Gerät vom Netzwerk zu trennen
 - Den Besitzer des Datenträgers befragen, welche Daten darauf gespeichert waren
 - Passwörter ändern / betroffene Accounts sperren

Datenrettung

- Beispiele:
 - Ein Mitarbeiter kann plötzlich eine sehr wichtige Office-Datei nicht mehr auf seinem Laptop finden
 - Eine Festplatte ist heruntergefallen und der PC bootet nun nur noch mit Fehlermeldungen
 - Ransomware hat zugeschlagen
- Was man als Ersthelfer tun kann:
 - Am betroffenen PC nicht mehr weiterarbeiten
 - Keine laienhaften Datenrettungsversuche
 - VM? System eventuell „pausieren“
 - Backups prüfen
 - Forensische Kopie erwägen

Infizierte Systeme (Malware, Ransomware, ...)

■ Beispiele:

- Ein Mitarbeiter hat aus privater Motivation eine Software aus dem Internet installiert („Raubkopie“) -> diese hat ein „Überraschungsei“ mitgebracht
- „Klassiker“: E-Mail mit „Bewerbung.zip“ und anschließender Crypto-Ransomware
- Drive-by-Download
- Zielgerichteter Angriff

■ Was man als Ersthelfer tun kann:

- Betroffene Systeme/Netzsegmente in Quarantäne setzen (vom Netzwerk trennen)
- Nicht einfach ausschalten
- Auf keinen Fall „bereinigen“
- Nach dem „Patient 0“ Ausschau halten, Benutzer befragen und dokumentieren, was wann passiert ist

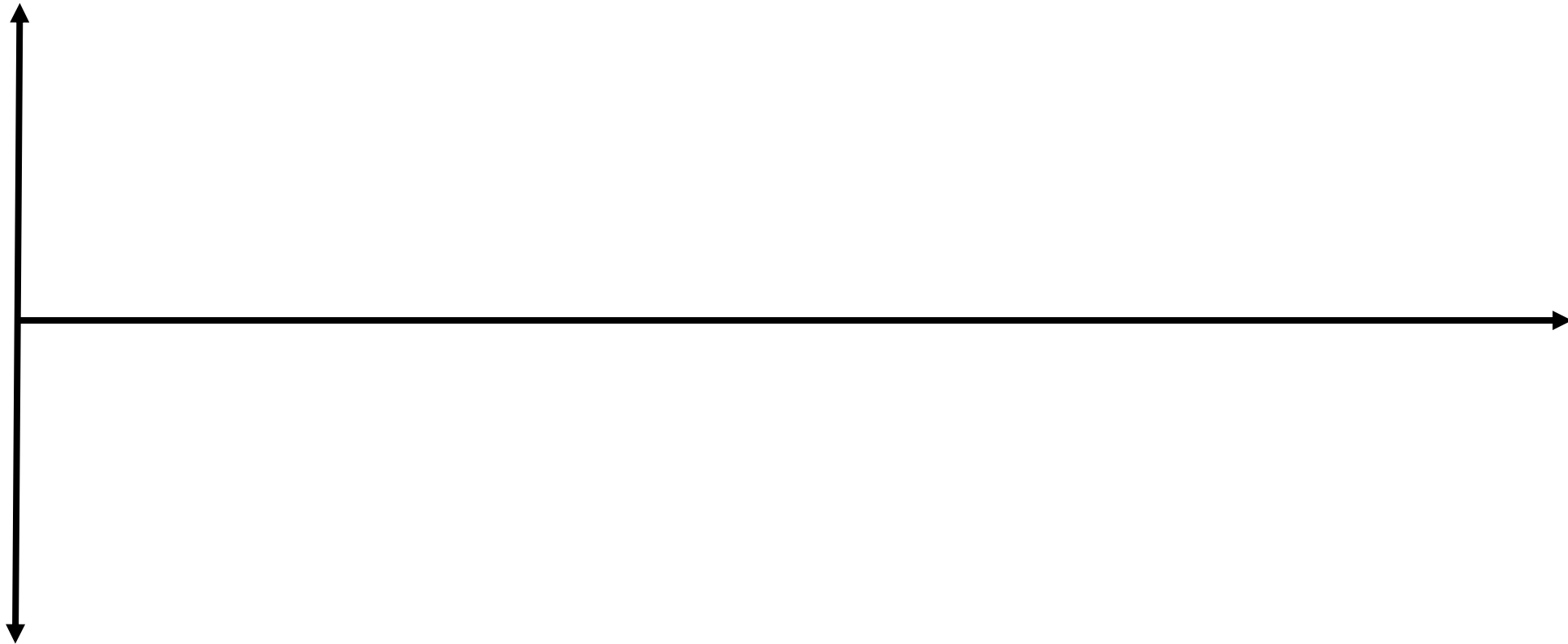
Denial of Service (DoS/DDoS)

- Beispiele:
 - Politisch motivierte Täter haben sich zusammengetan, um Ihr Unternehmen an seiner IT-gestützten Geschäftsausführung zu hindern (Stichwort: „LOIC“)
 - Erpressungsversuch
 - Der Server-Axt-Mörder
- Was man als Ersthelfer tun kann:
 - Prüfen ob es ein Störfall ist, oder ein Sicherheitsvorfall
 - Prüfen, wie wichtig der Internetuplink ist
 - Alternativen Kommunikationskanal erwägen (z.B. Tethering)
 - Eventuell einfach Ressourcen erhöhen (mehr Leitungskapazität)

Cyberstalking

- Beispiele:
 - Ein(e) Kolleg*in erhält E-Mails mit Morddrohungen und der Ankündigung, intime Details über sie zu veröffentlichen; später gehen solche Mails auch an Kollegen
 - Der Messenger-Account eines Mitarbeiters wurde gehackt. Darüber werden nun in seinem Namen „schlüpfrige“ Aufforderungen an Kolleginnen gesendet
- Was man als Ersthelfer tun kann:
 - Darauf achten, dass E-Mails inkl. aller Header gesichert werden (z.B. abfotografieren oder ausdrucken)
 - Bedenken, dass es sich für die Betroffenen um eine außerordentlich belastende Situation handeln kann
 - Mit dem Betroffenen ein genaues „Tagebuch“ über die Ereignisse beginnen

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



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

Security Information and Event Management (SIEM)

- **SIEM** kombiniert zwei Konzepte:
 - Security Information Management (SIM)
 - Security Event Management (SEM)
- **Zweck:**
 - Analyse (zeitnah oder sogar in Echtzeit) von Events/Alarmen aus Anwendungen/Netzwerk/Infrastruktur/...
 - Im Bereich IT-Sicherheit

“Digitaler Ersthelfer”

- Darüber hinaus soll der Begriff **Digitale Ersthilfe** wie folgt verstanden werden:
 - 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.

High-Level-Betrachtung

Was ist Incident Response?

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

Kernaktivitäten:

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

Definition und Motivation

"Unter den Begriff 'Incident Response' (...) fallen alle Aufgaben und Funktionen, die mit der Reaktion auf Vorfälle in einem konkreten technischen oder organisatorischen Zusammenhang stehen.,,

(Dr. Klaus-Peter Kossakowski: Information Technology - Incident Response Capabilities, S. 13)

- Gutes Incident Response kann Schäden und Folgeschäden minimieren und damit letztlich Kosten reduzieren
- Oft auch geringere Wahrscheinlichkeit zukünftiger Ereignisse (bei weiteren Bestrebungen)

WIE ERKENNE ICH EINEN IT-SICHERHEITSVORFALL?

Kurz gesagt: Nicht jedes auffällige Ereignis ist auch ein Sicherheitsvorfall. Ernst wird die Lage aber meist dann, wenn

- ! die **Vertraulichkeit** Ihrer Daten nicht mehr gewährleistet ist (Jemand hat ihre Daten „geklaut“, oder Sie haben aus Versehen eine wichtige E-Mail an einen falschen Empfänger versendet.)
- ! die **Verfügbarkeit** betroffen ist (Ihr wichtiger E-Commerce-Server ist plötzlich nicht mehr erreichbar, oder eine Festplatte mit kritischen Daten ist defekt.)
- ! die **Integrität** nicht mehr gewährleistet ist (Plötzlich stimmt Ihre Buchhaltung nicht mehr, oder einer Ihrer Computer ist von einem Trojaner befallen.)

Vorschläge („klare Fälle“) für die verschiedenen Kritikalitätsstufen

■ HOCH

- Alte Software oder Firmware Version entdeckt, die eine bekannte ausnutzbare Schwachstelle besitzt
- Die Admin-Nutzerkontodaten sind frei verfügbar (z.B.: abgelegt auf dem Netzwerk-Share, Standard-Passwort)
- Höhere Rechte als notwendig an Nutzer vergeben (z.B.: administrative Rechte für einen normalen Nutzer)
- Ein nicht lokales, administratives Konto, auf welches ein normaler Nutzer zugreifen kann (Active-Directory-Admin, Hypervisor/ESXi-Admin, Router, UPS ...)
- Unautorisierte Person im Server-Raum
- Verfügbarkeit von geschäftskritischen Systemen ist eingeschränkt, vor allem während Zeiten hoher Nachfrage
- Unbekannte/Unerwartete Prozesse auf einem Server
- Verlust eines unverschlüsselten Speichermediums (inklusive Laptops) mit internen Daten
- Malware auf einem Server-System
- Webseiten-Defacement oder eine ausnutzbare Schwachstelle auf dieser (z.B.: SQL-Injection, Cross-Site-Scripting)

Vorschläge („klare Fälle“) für die verschiedenen Kritikalitätsstufen

■ MITTEL

- Unbekannter Prozess auf einem Client-Computer
- Unerwartet schnell öffnendes und schließendes Konsolen-Fenster auf einem Client-Computer
- Standard oder triviale Anmeldedaten auf Peripheriegeräten (Drucker, Handy, ...)
- Ausweitung von Benutzerrechten auf andere, gleich privilegierte Konten
- Ein dringlicher legitimer Zugriff ist nicht möglich
- Unverschlossenes Server-Rack an einem öffentlich zugänglichen Ort oder unverschlossener IT-Raum

Vorschläge („klare Fälle“) für die verschiedenen Kritikalitätsstufen

■ **NIEDRIG**

- Verlust verschlüsselter Speichermedien (inklusive Laptops) mit internen Daten
- Alte Software oder Firmware Version entdeckt, die keine ausnutzbare Schwachstelle besitzt

■ **UNTERSTÜTZUNG/EVENT**

- Nutzer hat ein Passwort vergessen
- Ein einzelner legitimer Nutzer kann sich nicht einloggen (ohne hohe Dringlichkeit)

Grobe Klassifikationshilfe für die Kritikalitätsstufe „HOCH“

- Kann/wird jemand (deswegen) sterben?
- Droht (deswegen) Insolvenz?
- Kann/wird (deswegen) jemand ins Gefängnis kommen?

Aus dem Rheinischen Grundgesetz

Artikel 1: Et es wie et es.

Artikel 2: Et kütt wie et kütt.

Artikel 3: Et hätt noch emmer joot jejange.

Artikel 6: Kenne mer nit, bruche mer nit, fott domet.

Artikel 7: Wat wells de maache?

*Oder nüchtern sachlich: es gibt nicht den goldenen Weg und
Ziele müssen unter Unklarheit abgewogen werden*

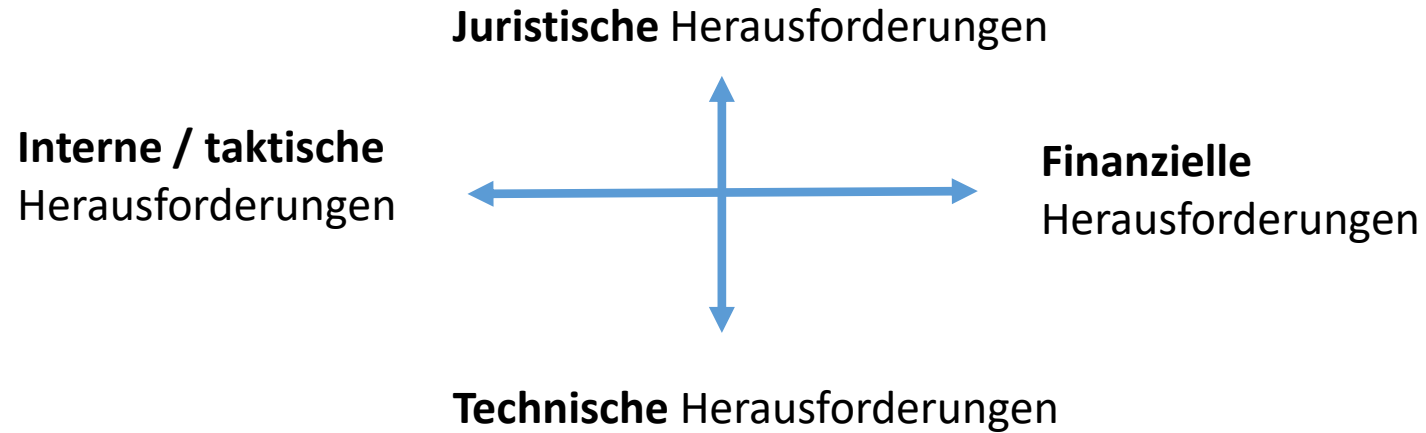
Ziele und Verantwortung

Ziele können sich ergänzen, oder gegenseitig behindern

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

Verantworten muss letztlich der Geschäftsführer

Herausforderungen aus Sicht des verantwortlichen CEO/CIO



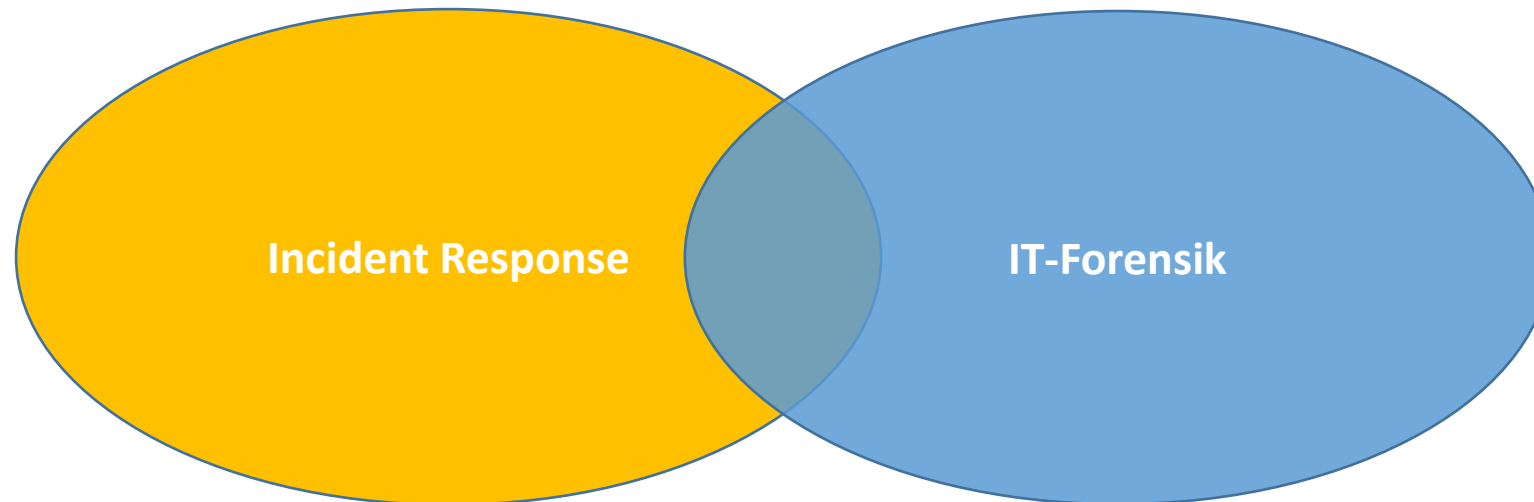
W-Fragen

W-Fragen

- Wo ist etwas passiert?
- Was ist geschehen?
- Wann ist es passiert?
- Welche Daten sind betroffen?
- Welche Systeme sind betroffen?
- Welche Mitarbeiter/Kunden sind betroffen?
- Wer hilft mir als GF wie, wann, wo?
- Welche Priorität gebe ich dem Fall?
- Welche Maßnahmen müssen unmittelbar umgesetzt werden?
- ...

Schnittmenge und Abgrenzung

- Hauptunterschied: Zielsetzung



IT-Forensik im Rahmen von Incident Response

Quelle: BSI-Leitfaden IT-Forensik,
S. 14

- **Incident Response:** Vorfallsbearbeitung, insbesondere Krisenreaktion auf einen IT-Sicherheitsvorfall
- **Notfallmanagement**
 - **Vorfallsbearbeitung:**
 1. **Sofortmaßnahmen** (die eigentliche **Krisenreaktion**): Erfüllung unmittelbarer und dringlicher Aufgaben, Schadensbegrenzung, Kosten in dieser Phase noch untergeordnet
 2. **Wiederaufbau** (recovery): Notfallbetrieb mit eingeschränkten Ressourcen, Vermeidung/Begrenzung von Folgeschäden, in ruhigeres Fahrwasser gelangen
 3. **Wiederherstellung** (restauration): Zustand vor dem Ereignis wiederherstellen, alle Auswirkungen beseitigen, Normalbetrieb sicherstellen
 - **IT-Forensische Maßnahmen** zu 1.-3. über den gesamten Verlauf der Krise erforderlich
 - Oft **Zielkonflikt** Aufklärung vs. Wiederherstellung, Untersuchung vs. Betrieb

IT-Forensik im Rahmen von Incident Response

Quelle: BSI-Leitfaden IT-Forensik,
S. 14

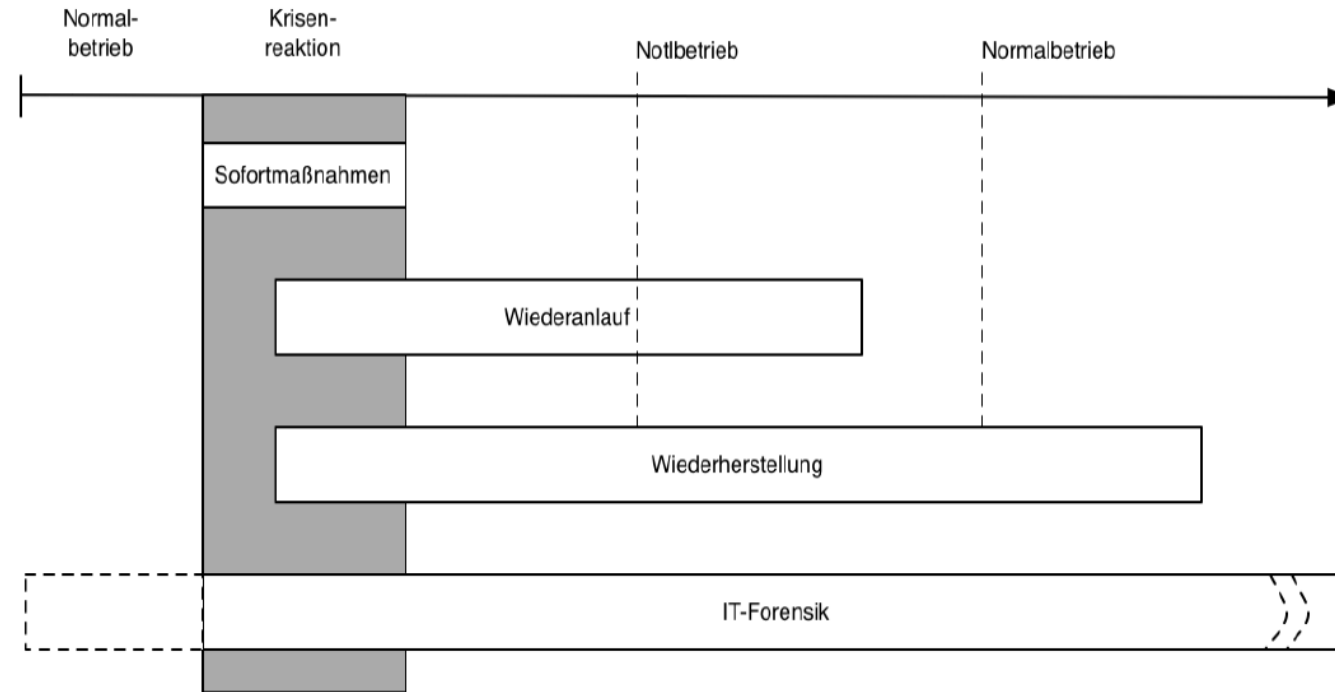
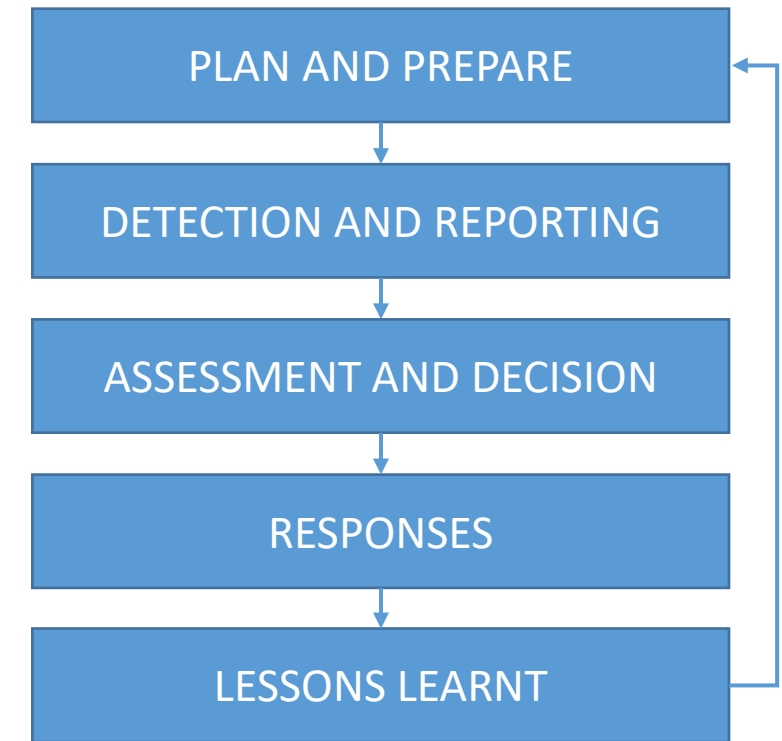


Abb. 1: Zeitliche Einordnung der Krisenreaktion nach [Rös03] mit Hinzunahme der IT-Forensik

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

- 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



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

- **Planen und Vorbereiten**
 - Gründung eines IT-Sicherheit-Incident-Managements + Team oder Digitaler Ersthelfer, Erschaffung und Fortentwicklung z.B. von Leitlinien, Plan testen, ...
- **Erkennen und Melden**
 - System- und Netzwerküberwachung, erkennen von böartigen Events, Berichten relevanter Events, ...
- **Bewertung und Entscheidung**
 - Sammeln weiterer Informationen, bewerten und entscheiden zum klassifizieren als Event oder Incident, ...
- **Rückmeldungen**
 - Eindämmung, Wiederherstellung, Auflösung des Incidents, ...
- **Gewonnene Erkenntnisse**
 - Identifikation der gewonnenen Erkenntnisse, Nachbesprechung, Evaluation der Performance und Effektivität, ...

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**

Zwingend notwendiges „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

Information Security Event / Incident Report Form
No. 7 - 19, only applicable when Event is escalated to an Incident | Page 1/10

DigiTrace
Kompetenz in IT-Forensik

DigiTrace
Kompetenz in IT-Forensik

Information Security Event / Incident Report Form
Version: 0.4 | 20th of January 2020

Purpose: This document serves as a template and is adjustable to your own needs. You can fill it out on paper or use it on your computer.

Audience: Digital first responders, IT-security and computer forensic experts. Everyone who needs to report an IT event / incident.


DigiTrace GmbH
Zollstockgürtel 59
50969 Köln
Tel.: +49 221 6778695-0
info@digiTrace.de
www.DigiTrace.de

Lizenz: CC BY-SA 3.0 DE

1/10

Zwingend notwendiges „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

- Die folgenden „Regeln“ gelten im Sinne von „Goldenen Regeln“ als bewährte und zugleich abstrakte Verhaltenstipps für jeden Digitalen Ersthelfer:
 1. Seien Sie als Ansprechpartner für Ihre Kolleg*innen greifbar.
 2. Wirklich niemand weiß alles, aber Dinge ernst nehmen, kann oft Schlimmeres verhindern. Denn ein Fehlalarm ist besser, als ein übersehener Ernstfall.
 3. Nichts "auf die lange Bank schieben" – sorgen Sie dafür, dass jemand der Quellursache auf den Grund geht.
 4. Ruhe bewahren und nach Möglichkeit Ruhe ausstrahlen.
 5. Events/Incidents von Beginn an konsequent und lückenlos dokumentieren.
 6. Beachten Sie die sieben W-Fragen: Wer? Was? Wann? Wo? Warum? Wie? Wozu?
 7. Prüfen/Hinterfragen Sie unverzüglich, ob Backups vorliegen, sicher und vollständig sind.
 8. Eingeschaltete Geräte bleiben eingeschaltet, ausgeschaltete Geräte bleiben ausgeschaltet.
 9. Begrenzen Sie Änderungen an (betroffenen) Systemen auf das absolute Minimum.
 10. Ziehen Sie, wenn angebracht, (externe) Experten hinzu (IT-ler, IT-Forensiker, Juristen, PR-Experten, ...).

Wiederkehrende, vorlesungs- und übungsbegleitende Übungsaufgabe

- Überarbeiten Sie Ihre Planung für die Errichtung einer „smarten“ Einbruchmeldeanlage 2.0 für das Handwerksunternehmen Ihrer Eltern
- Beantworten und begründen Sie unter eigenen Annahmen z.B. folgende Fragen:
 - Ändern Sie Ihre bisherige Planung?
 - Welche IT-Vorfälle können grundsätzlich in Ihrer Anlage (und auch im Unternehmen selbst) auftreten? Wie schätzen Sie die Wahrscheinlichkeit jeweils ein? Können Sie Beispiele finden für IT-Vorfälle in den Kritikalitätsstufen Niedrig/Mittel/Hoch?
 - Skizzieren Sie mögliche Problemstellen. Wo könnten Probleme lauern?