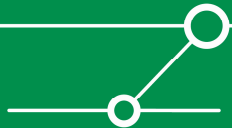


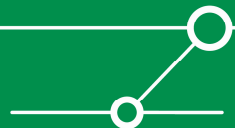
Incident Response & Human Errors – What we can learn from the Titanic

**Enno Rey, erey@ernw.de
CISSP/ISSAP, CISA**

Friedwart Kuhn, fkuhn@ernw.de

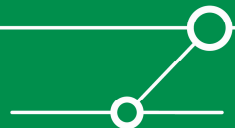


- **Gegründet Sommer 2001 durch Enno Rey**
- **Netzwerk-Dienstleister mit Sicherheits-Fokus**
- **Aktuell zwölf Mitarbeiter**
- **Schwerpunkte: Security Management, Audit/Revision, Penetrations-Tests, Security Research**
- **Kunden (Europa/USA):
Industrie, Banken, Behörden, Provider**



Agenda

- **Überblick & Einführung *Incident Response***
- **Human Errors – ein etwas akademischer Exkurs**
- **Die Titanic und was wir davon lernen können**



Incident Response – Versuch einer Definition

■ Incident Response...

...ist eine Menge bestehend aus Definitionen, Kategorien, Prozessen und Verfahren, um mögliche sicherheitsrelevante Vorfälle zu entdecken, strukturiert zu berichten, zu beheben und um künftigen Vorfällen geeignet vorzubeugen

■ Definitionen

- ...von verwendeten Begrifflichkeiten wie 'incident', 'event' und anderen
- ...von Verantwortlichkeiten

■ Kategorien

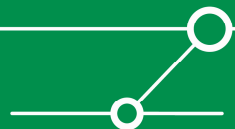
- ...von incidents

■ (organisatorische) Prozesse

- z. B. wer wem wie berichtet

■ (technische) Verfahren

- z. B. zum Reporting oder zur forensischen Analyse



■ Event

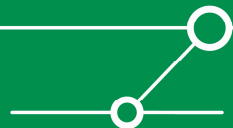
- "An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant." (Abschnitt 3.2 ISO 18044)

■ Incident

- "An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security." (Abschnitt 3.3 ISO 18044)

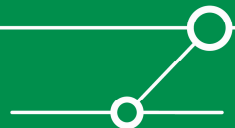
■ ISIRT

- "An ISIRT is a team of appropriately skilled and trusted members of the organization, which will handle information security incidents during their lifecycle. At times this team may be supplemented by external experts, for example from a recognized computer incident response team or Computer Emergency Response Team (CERT)." (Abschnitt 3.4 ISO 18044)

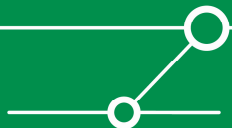


Der Incident Response-Prozess

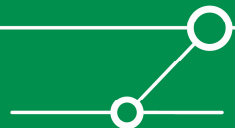
- **Auf einer sehr hohen Ebene besteht der Incident Response-Prozess aus vier Phasen (ISO 18044) in Analogie zum PDCA-Modell (ISO 27001)**
- **Planung und Vorbereitung**
 - z. B. Incident Response-Policy; Formulare für Vorfälle
- **Umsetzung**
 - z. B. Entdecken und Berichten von Vorfällen; geeignetes Reagieren auf Vorfälle
- **Review**
 - z. B. Analyse dessen, was zu dem Vorfall geführt hat
- **Verbesserung**
 - z. B. Lessons learned und Implementierung der Veränderungen



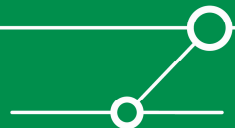
- **Vorbereitung (Preparation)**
- **Entdeckung und Analyse (Detection and Analysis)**
- **Schadensbegrenzung, -behebung und Wiederherstellung (Containment, Eradication and Recovery)**
- **Post-Incident-Aktivität (Post-Incident Activity)**



- **Definition Incident Response-Policy**
 - Einleitung & Scope
 - Aussage /Zweck der Policy
 - Incident Response-Prozesse und –Verfahren
 - Definition von Verantwortlichkeiten
 - Dokumentation und Verweise
 - Durchsetzung
 - (Appendix)
- **Definition von Incident-Kategorien**
- **Einrichtung einer Incidence Response-Struktur gemäß der Incident Response-Policy in der Organisation**
 - d. h. vor allem Definition und Implementierung von Incident-Handling- und –Kommunikationsvorrichtungen Hardware- und Software-Ressourcen
 - in größeren Organisationen bedeutet das meistens die Implementierung eines ISIRT (Information Security Incident Response Team)



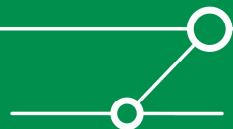
- **Mögliche Incident-Kategorien (für jede Organisation zu vervollständigen)**
- **...gemäß ISO 18044**
 - Denial of Service
 - Information Gathering
 - Unauthorized Access
- **...zusätzlich gemäß NIST SP 800-61**
 - Malicious Code
 - Inappropriate Usage
 - Multiple Component



Teilprozess – Vorbereitung

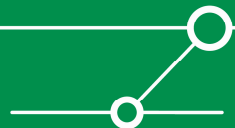
- **Tools & Ressourcen für das Incident-Handling**
(aus dem Computer Security Incident Handling Guide des NIST SP 800-61)

Acquired	Tool / Resource
Incident Handler Communications and Facilities	
	Contact information for team members and others within and outside the organization (primary and backup contacts), such as law enforcement and other incident response teams; information may include phone numbers, e-mail addresses, public encryption keys (in accordance with the encryption software described below), and instructions for verifying the contact's identity
	On-call information for other teams within the organization, including escalation information (see Section 3.2.6 for more information about escalation)
	Incident reporting mechanisms, such as phone numbers, e-mail addresses, and online forms that users can use to report suspected incidents; at least one mechanism should permit people to report incidents anonymously
	Pagers or cell phones to be carried by team members for off-hour support, onsite communications
	Encryption software to be used for communications among team members, within the organization and with external parties; software must use a Federal Information Processing Standards (FIPS) 140-2 validated encryption algorithm ¹¹
	War room for central communication and coordination; if a permanent war room is not necessary, the team should create a procedure for procuring a temporary war room when needed
	Secure storage facility for securing evidence and other sensitive materials
Incident Analysis Hardware and Software	
	Computer forensic workstations ¹² and/or backup devices to create disk images, preserve log files, and save other relevant incident data
	Laptops, which provide easily portable workstations for activities such as analyzing data, sniffing packets, and writing reports
	Spare workstations, servers, and networking equipment, which may be used for many purposes, such as restoring backups and trying out malicious code; if the team cannot justify the expense of additional equipment, perhaps equipment in an existing test lab could be used, or a virtual lab could be established using operating system (OS) emulation software
	Blank media, such as floppy diskettes, CD-Rs, and DVD-Rs
	Easily portable printer to print copies of log files and other evidence from non-networked systems
	Packet sniffers and protocol analyzers to capture and analyze network traffic that may contain evidence of an incident
	Computer forensic software to analyze disk images for evidence of an incident
	Floppies and CDs with trusted versions of programs to be used to gather evidence from systems
	Evidence gathering accessories, including hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape, to preserve evidence for possible legal actions
Incident Analysis Resources	
	Port lists, including commonly used ports and Trojan horse ports
	Documentation for OSs, applications, protocols, and intrusion detection and antivirus signatures
	Network diagrams and lists of critical assets, such as Web, e-mail, and File Transfer Protocol (FTP) servers
	Baselines of expected network, system and application activity
	Cryptographic hashes of critical files ¹³ to speed the analysis, verification, and eradication of incidents



■ **Verhinderung von Incidents durch Vorbeugen**

- Verhinderung ist nicht Kernaufgabe, aber gleichwohl Teilprozess
- Wichtige Methode der Vorbeugung ist eine regelmäßige Risikoanalyse mit Risikobewertung, um potentielle(n) Incidents erkennen (vorbeugen) zu können
 - ⇒ Schnittstelle zur Risikoanalyse
- Implementierung von Sicherheitsprinzipien
 - User Awareness
 - Least Privilege
 - Minimal Machine
 - Patchmanagement
 - Starke Authentifizierung
 - Secure the weakest Link
 - Defense in depth
 - Segregation of Duties
 - Nachvollziehbarkeit



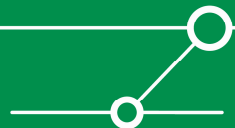
■ **Entdeckung des Incidents & Reporting**

- automatisch, z. B. via IDS, AV-Software, regelbasierte Loganalyse
- manuell z. B. dadurch, dass Anomalien auffallen (gewöhnlicher Benutzer vs. Spezialist)
- Report-Verfahren und -Struktur

■ **Einordnung in eine Incident-Kategorie (s. o.)**

■ **Dokumentation /Erfassung des Incidents**

- Status, Beschreibung, bisher unternommene Aktionen, Kontaktinformationen für involvierte Parteien, Liste gesammelter Beweismittel, nächste zu unternehmende Schritte

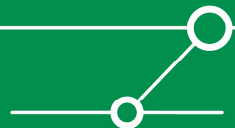


■ Analyse des Incidents

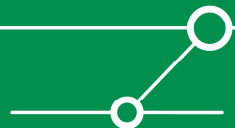
- ...durch das CERT /SIRT oder dafür vorgesehene und definierte Verantwortliche z. B. durch:
 - Analyse von Logs (betroffene Systeme & Applikationen, Routern und Firewalls)
 - Vergleich von Incident-Logs mit 'gewöhnlichen' Logs (Voraussetzung: Profiling von Systemen)
 - wenn möglich und wenn ein Prozess dafür existiert: forensische Analyse

■ Priorisierung des Incidents (unter Zugrundelegung folgender Kriterien)

- aktuelle und potentielle Schadenswirkung des Incidents
- Kritikalität der /des betroffenen Ressource /Systems



- **Entscheidung für eine Strategie zur Schadensbegrenzung (zur Klärung von Fragen wie z. B.: soll ein Webserver mit einer infizierten Webseite abgeschaltet werden /isoliert werden /der Zugriff auf die infizierte Seite unterbunden werden??) unter Zugrundelegung folgender Kriterien**
 - dabei möglicher Schaden für das System /die Ressource /Applikation
 - Folgen des Abschaltens oder Isolierens des Systems /der Ressource /Applikation
 - Notwendigkeit der Beweissicherung
 - Zeit und Ressourcen für die Implementierung der Strategie
 - Effektivität der Strategie
 - ...

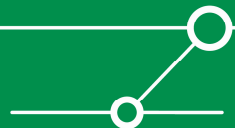


■ Schadensbehebung und Wiederherstellung

- ...sind meistens OS- oder Applikations-spezifisch
- Wenn nötig /möglich Einleitung von Maßnahmen zur Entfernung von Schadcode (Bsp.: Virus vs. Rootkit!)
- Einspielung von aktuellsten Backups

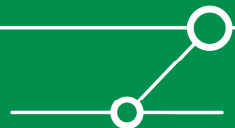
⇒ Es gibt Schnittstelle zu Business Continuity

⇒ Es gibt Schnittstelle zu Disaster Recovery



■ Lessons Learned

- extrem wichtig für künftige Verbesserungen
- z. B. durch ein Post Incident-Meeting zwischen allen involvierten Parteien zur Behandlung von Fragen wie
 - Was passierte genau, warum und zu welcher Zeit?
 - Performance der Reaktion des Teams (CERT /ISRT /'Incident-Handlers')?
 - Wie würde das Team jetzt bei identischem Vorfall handeln?
 - Welche Informationen wären eher benötigt worden?
 - Welche korrigierenden Maßnahmen auf Designebene, organisatorischer oder technischer Art sollten für künftige Vermeidung des Vorfalls implementiert werden?
 - Welche Tools & Ressourcen sind für eine effektivere Entdeckung, Klassifikation, Analyse und Schadensminderung künftig notwendig?
 - ...

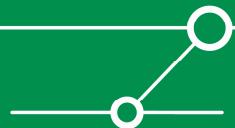


- **Aufbewahrung /Speicherung der gesammelten Daten**

- ...um künftig effektiver reagieren zu können
- ...um Beweismaterial zu besitzen

...unter Berücksichtigung einer (zu definierenden) Policy für Aufbewahrungsdauer und Vertraulichkeit(sklassifizierung) gemäß den Kriterien:

- mögliche strafrechtliche Relevanz
=> Schnittstelle zu Legal Compliance
- Kosten /Aufwand



Putting all together...

- Incident Response-Flussdiagramm aus ISO 18044

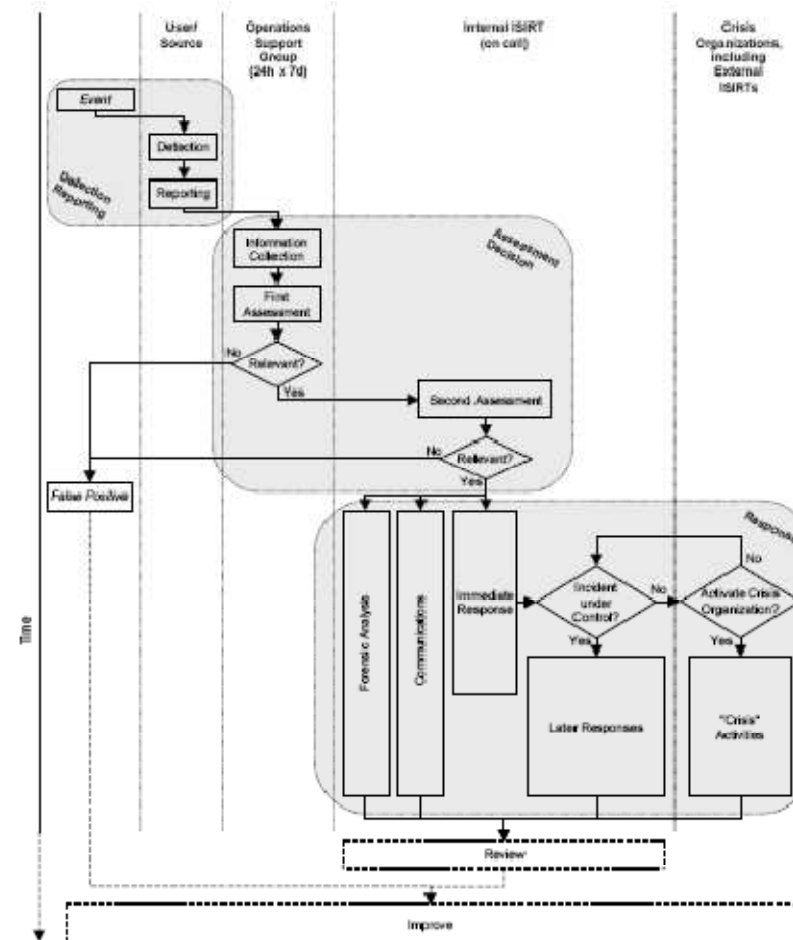
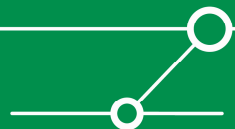
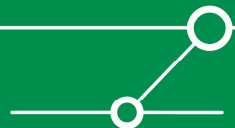


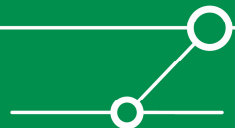
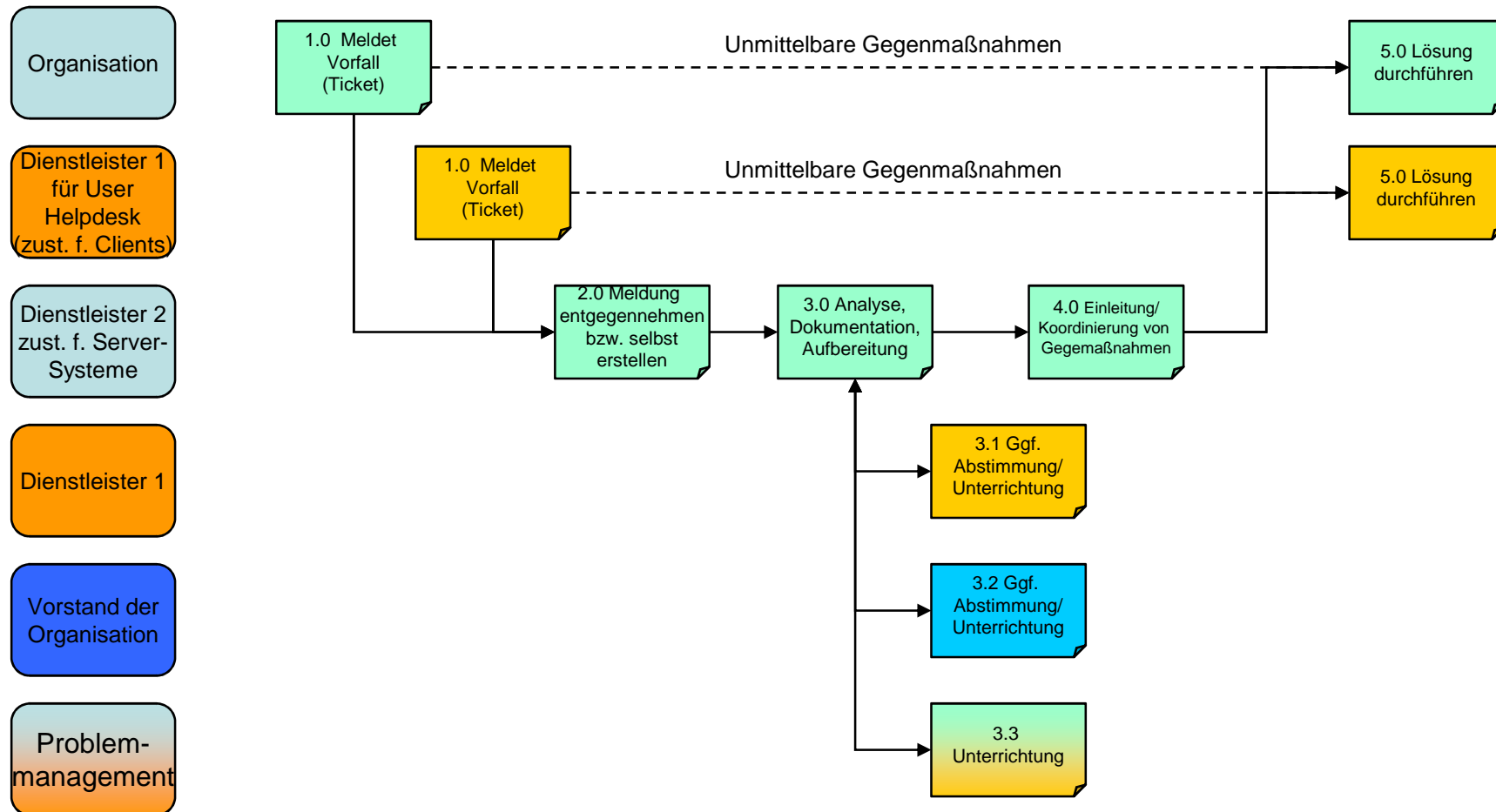
Figure 2 - Information Security Event and Incident Flow Diagram



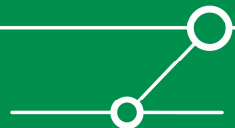
- **Grundsätzlich gilt für jeden Teilprozess des Incident Response-Prozesses die Einhaltung rechtlicher und betrieblicher Rahmenbedingungen (zusammengefasst unter 'Legal Compliance' in BS /ISO 17799)**
 - **Es gibt Schnittstellen zu anderen Teilprozessen eines ISMS, besonders zur übergeordneten ISO 17799:**
 - (immer) Compliance (s. o. – Abschnitt 15)
 - Risikoanalyse (Abschnitt 4)
 - High Level Security Policy (Abschnitt 5)
 - Business Continuity (Abschnitt 14)
 - Disaster Recovery (Abschnitt 14)
- und im weiteren Sinne auch zu:**
- Operations and Communications Management (Abschnitt 10)
 - Information Systems Acquisition, Development and Maintenance (Abschnitt 12)



Diskussionsbeispiel: Incident Response- Prozessablauf bei einem Finanzinstitut

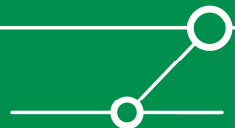


- **[1] ISO /IEC TR 18044 Information technology – Security techniques – Information security incident management**
- **[2] BS ISO /IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management**
- **[3] ISO/IEC 27001:2005 - Information technology – Security techniques -- Information security management systems – Requirements**
- **[4] NIST Special Publication 800-61 – Computer Security Incident Handling Guide**
- **[5] SANS Institute – Computer Security Incident Handling. Step by Step**



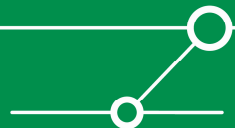
Active vs. Latent Failures

- **Active failures** are unsafe acts committed by those at the “sharp end“ of the system (pilots, air traffic controllers, ships‘ crews, train drivers, control room operators, maintenance crew and the like). They are the people at the human-system interface whose actions can, and sometimes do, have immediate adverse consequences. Quite often, these unsafe acts involve the circumvention or disabling of engineered safety devices designed to defend the system against serious breakdowns.
- **Latent failures** are usually fallible decisions, taken at the higher echelons of the organization, whose damaging consequences may lie dormant for a long time, only becoming evident when they combine with local triggering factors (i.e., active failures, technical faults, atypical system states, etc.) to breach the system‘ s defenses.



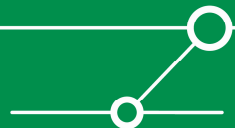
Active vs. Latent failures in IR

- **Versuchen Sie stets, zu verstehen, welche *Latent Failures* möglicherweise am Entstehen eines Incidents beteiligt waren!**
- **=> ggf. Aufnahme dieser Bewertung in IR-Prozess und -Dokumente. Dies setzt entsprechendes Training der beteiligten Personen voraus.**

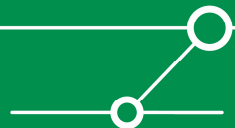


Active Human Error Forms

- **Skill Based**
 - Know what you're doing
- **Rule Based**
 - Think you know what you're doing
- **Knowledge Based**
 - Know you don't know what you're doing
 - => i.a. hier höchste Fehlerquote & Auswirkung

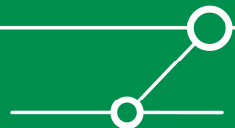


- **Diese Fehlerarten müssen unterschiedlich adressiert werden.**
- **=> eine Einordnung kann für den Post Incident Prozess *sehr* hilfreich sein.**



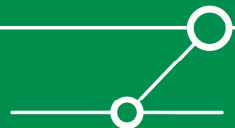
Types of Events (H.W. Heinrich)

- Misadventures
- No Harm Events
- Near Misses

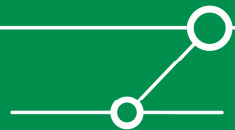


Types of Events

- **Misadventures:** The event actually happened and some level of harm – possibly death – occurred.
- **No Harm Events:** The event actually occurred but no harm was done.
- **Near Miss:** The potential for harm may have been present, but unwanted consequences were prevented because some recovery action was taken.

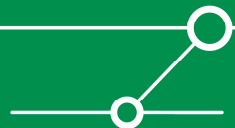


Near Miss



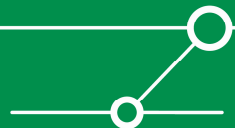
Konsequenzen für IR

- Zur Aufdeckung insbesondere von *Latent Failures* und *nachgelagerter* Verbesserung/Fehlervermeidung sollte ein Reporting von *No Harm Events* und *Near Misses* stattfinden.
- Dies ist in den meisten Organisationen *nicht* der Fall.



Why Near Misses should be reported

- **Prevent failure**
- **Make failure visible**
- **Prevent adverse effects of failure**
- **Mitigate the adverse effects**



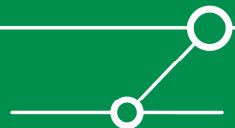
Four Major Reasons for Not Reporting



- **The error was fixed before anything bad happened.**
- **It's easier to just fix the error than tell anyone about it.**
- **The error might be written in a personnel file.**
- **Not wanting to get themselves or anyone else in trouble.**

- **=> i.a. langfristige organisatorische Änderungen (und etwa entsprechendes Training) notwendig.**

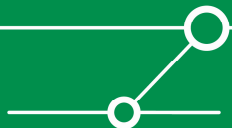
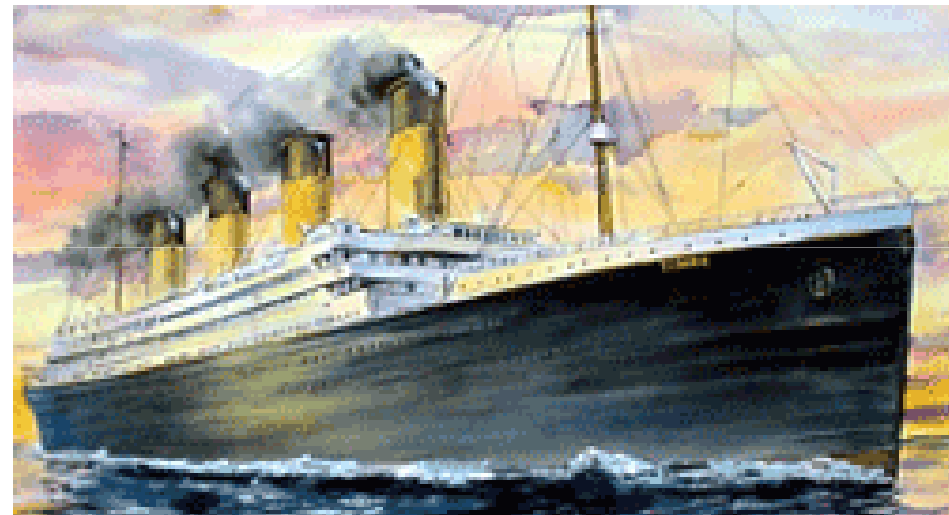
- **Dafür effektive & nachhaltige Verbesserung und Verringerung der Wahrscheinlichkeit des Eintretens eines Desasters und Verringerung des Schadens *bei* Eintritt.**



The Titanic

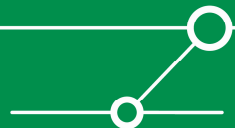
- **Grösstes Schiff der Zeit:**
 - knapp 300 Meter lang
 - 25 Stockwerke hoch
 - 46.000 Tonnen schwer

**[Zur Zeit des Konstruktion
das größte je gebaute
„bewegte Objekt“.]**



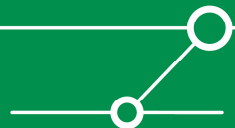
The Titanic

- Galt aufgrund von Bauweise als „unsinkbar“.
- Auf Jungfernfahrt Southhampton -> New York in der Nacht vom 14. auf 15. April 1912 Kollision mit Eisberg
- Schiff sinkt innerhalb von 2,5 Stunden
- Von über 2200 Passagieren überleben nur ca. 700.

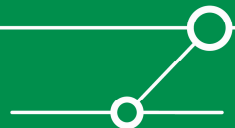


Ursachen für das *Desaster*

- **Design-Fehler**
- **Organisatorische/Prozedurale Probleme**
- **Unzureichende *Regulations*
[Legal Compliance war gegeben]**
- **Einige dieser Punkte sind stark umstritten
(nichtsdetrotz zur Diskussion aber gut geeignet).**



- **Titanic war in 16 *Compartments* aufgeteilt, deren einzelnes Fluten nicht das Sinken des Schiffs zur Folge haben sollte.**
- **Selbst bei Flutung mehrerer *Compartments* sollte ausreichend Zeit zur Herbeiholung von Hilfe vorhanden sein.**

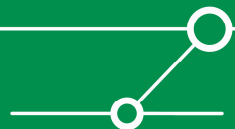
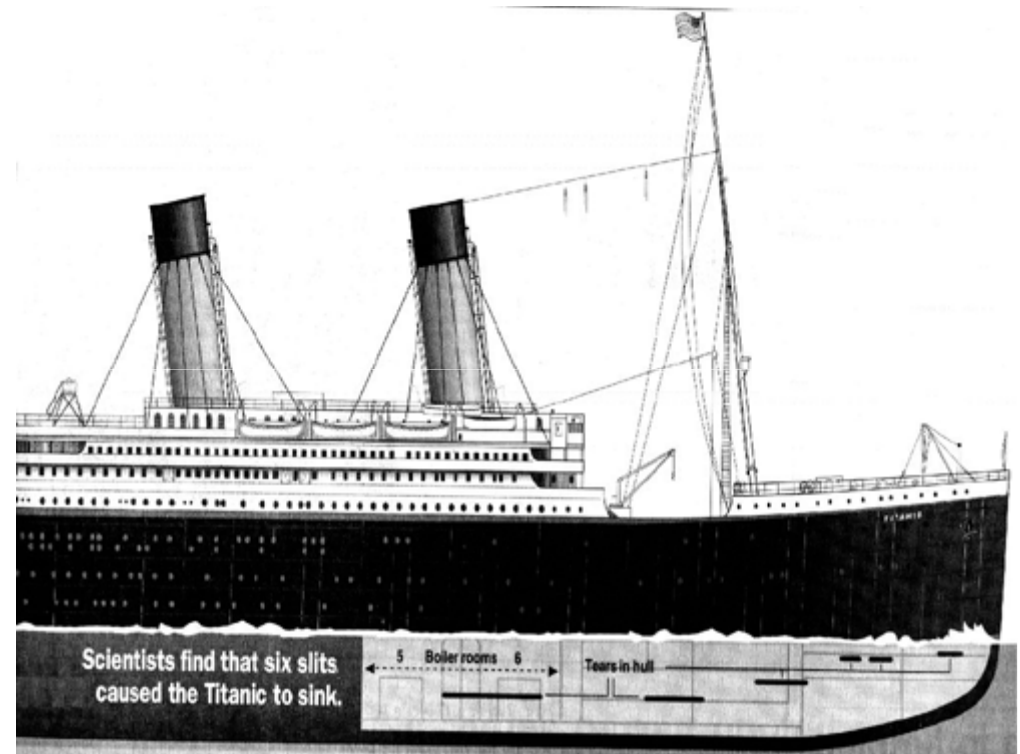


Design-Fehler – Compartments

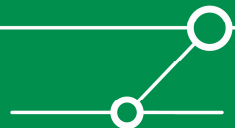
- **Compartments waren nach oben nicht dediziert schliessbar**

=> bei Neigung des Schiffs Übertritt von Wasser aus gefluteten Compartments in nicht-geflutete.

- **Lessons learned for IT Security?**



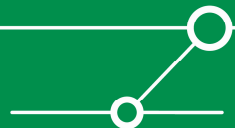
- **Unzureichende (Notfall-) Übung**
- **Schiff möglicherweise zu schnell unterwegs**
- **Kommunikations-Probleme**
- **Eisberg wird zu spät erkannt**
- **Falsche Reaktion auf Erkennung des Eisbergs**
- **Falsches Vorgehen hinsichtlich Information/Warnung**
- **Fehler bei Besteigen der Rettungsboote**



Unzureichende (Notfall-) Übung

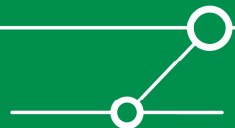
- **Es hatte keinerlei „Betriebs“- (oder sogar Notfall-Übung) stattgefunden.**
- **Ein Effekt war, dass Mann im Ausguck sein Fernglas nicht finden konnte.**

- ***Latent Failure***

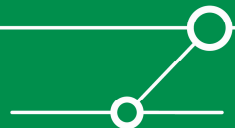


Schiff möglicherweise zu schnell unterwegs

- **Das Schiff war mit Volldampf unterwegs.**
- **Gemessen an Rahmenbedingungen (kein Wellengang, der auf Eisflächen hätte hinweisen können) diskussionswürdig.**
- **Ggf. Zusammenhang mit unzureichender Prozessierung von Eiswarnungen.**
- **Umstritten: Bruce Ismay wollte neuen Überfahrt-Rekord aufstellen.**
- **Ggf. Latent Failure
[falsche Risiko-Analyse/Goals]**



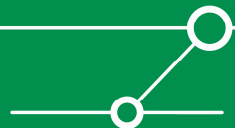
- **Funker wurde von Funktechnik-Ausrüster (Marconi) gestellt [Outsourcing ;-)]
=> suboptimale Kommunikation mit Brücke zu Eiswarnungen**
- **Funker stark mit privater Kommunikation beschäftigt**
- ***Latent Failure* (ungeeignete[s] Personal/Priorisierung)**



Eisberg wird zu spät erkannt

- **Lookout Fred Fleet hätte angesichts der Sichtverhältnisse Eisberg schon aus 1000 Yards (oder mehr) Entfernung sehen können**
- **... wenn er ein Fernglas zur Verfügung gehabt hätte**
- **... das (für ihn) unauffindbar war**

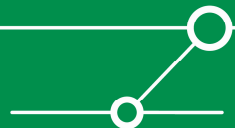
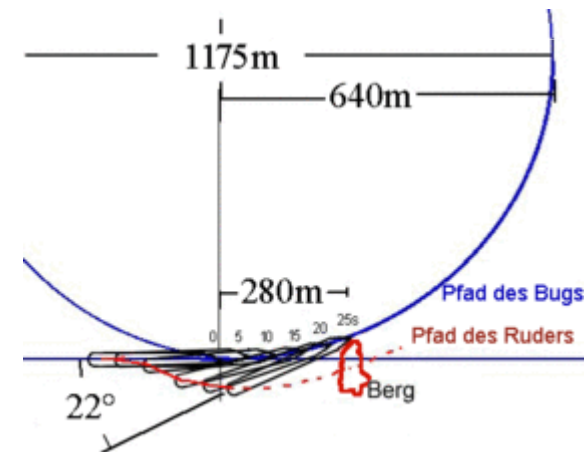
- **Latent Failure (s.o.)**
- **Active Failure?**
[Knowledge Based]



Falsche Reaktion

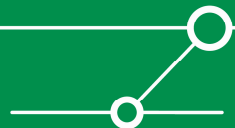
- **Officer Murdoch reagiert mit Anweisung: „Wenden!“
[Maschinen rückwärts]**
- **Schwerfälliges Manöver**
- **=> Schiff rammt Eisberg von der Seite**

- **Active Failure**
 - Rule based
 - Knowledge based



Falsches Vorgehen hinsichtlich Information/Warnung

- **Untere Stockwerke werden nur unzureichend informiert**
 - **Flucht wird erschwert/verspätet**
 - **Orchester spielt weiter, um Panik zu vermeiden**
-
- **Active Failure**
- Rule based

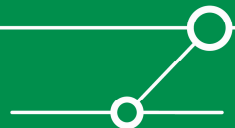


Fehler bei Besteigen der Rettungsboote



- **Rettungsboote werden teilweise nicht gefüllt, aufgrund von Regel „nur Frauen und Kinder“**

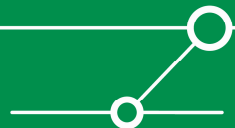
- **Active Failure**
- Rule based



Unzureichende *Regulations*

- **Schiff hatte deutlich zu wenig Rettungsboote an Bord**
- **Schiffseigner hatte Anzahl aus „ästhetischen Gründen“ reduziert**
- **Sie war aber innerhalb geltender Vorschriften (die nicht an Passagieranzahl, sondern Tonnage ausgerichtet waren).**
- **=> Legal Compliance, aber keine Security (Safety)**

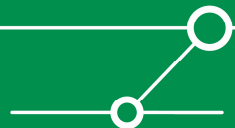
- **Latent Failure: unzureichende Disaster-Vorsorge (die eben vom *Disaster/Worst Case* ausgehen muss)**



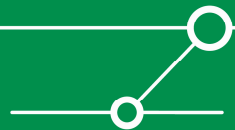
- Für den Untergang der Titanic sind (mit o.g. Vorbehalt) in erster Linie ***Active Failures*** verantwortlich.
- Für das daraus resultierende Desaster ***Latent Failures***.
- Die ***Active Failures*** fallen in die Kategorien ***Rule Based & Knowledge Based***.

- **Bessere Vorbereitung/Training/Prozesse hätten *möglicherweise* das Desaster verhindern können.**

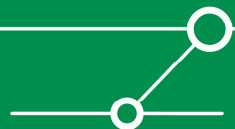
- **Hieraus können Lehren für die Wirksamkeit heutiger Incident Response Strukturen gezogen werden.**



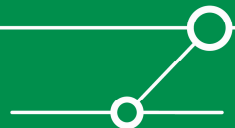
Fragen?



Danke für Ihre Aufmerksamkeit!



- **Wo sehen Sie Potential für *Latent Failures* beim Incident Handling in Ihrer Organisation?**
[sind die Prozesse beschrieben/mature?
sind die beteiligten Personen trainiert/ausreichend? etc.]
- **Sind in Ihren Incident Management Prozeduren Bestandteile zur Kategorisierung von Incident-/Fehlerursachen vorhanden?**
- **Definieren Sie Bestandteile (Dokumente, -teile, Ablaufschritte) zur Integration der Fehlerkategorisierung.**
- **Wie kann Reporting und/oder Organisationskultur hinsichtlich des Umgangs mit *Near Misses* optimiert werden?**



- **H.W. Heinreich & Dan Peterson: Industrial Accident Prevention, 5th Edition, 1980**

