

IT Forensik

Frankfurt, 14. Januar 2009
Gastvorlesung IT Forensik

Dr. Igor Podebrad
Threat Analysis & Forensic, Commerzbank AG

Overview / Agenda

- 1. Definition Begrifflichkeiten**
2. Rollen und Verantwortlichkeiten
3. Der IT-forensische Prozeß
4. Organisation und Vorbereitung einer IT-forensischen Untersuchung
5. Durchführung einer IT-forensischen Untersuchung
6. Abschluß und Nachbereitung einer IT-forensischen Untersuchung

Begriffe (1/5)

- **Information:**

- Informationen bilden im Besonderen den Inhalt einer Nachricht, in textlicher, grafischer oder audiovisueller Form. Informationen enthalten keine irrelevanten oder redundanten Teile. (Quelle www.itwissen.info)

- **Daten:**

- Daten sind in erkennungsfähiger Form dargestellte Elemente einer Information, die in Systemen verarbeitet werden können. Nach DIN 44300 sind Daten als Zeichen oder kontinuierliche Funktionen definiert, die aufgrund von bekannten oder unterstellten Abmachungen dem Zwecke der Verarbeitung dienen. (Quelle www.itwissen.info)

Begriffe (2/5)

- **Informationstechnologie / Informationstechnik (IT):**
 - Informationstechnik (IT) umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen. (Quelle BSI)
- **Sicherheitsziele:**
 - Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Nachvollziehbarkeit (Quelle Commerzbank)

Begriffe (3/5)

- **Informationssicherheit (IS):**

- Informationssicherheit hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. IT-Sicherheit beschäftigt sich an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Der Begriff "Informationssicherheit" statt IT-Sicherheit ist daher umfassender und wird daher zunehmend verwendet. (Quelle BSI)
- Der *Zustand eines IT-Systems*, in dem die damit verbundenen Risiken durch angemessene Sicherheitsmaßnahmen auf ein für die Organisation akzeptables Maß reduziert sind. (Quelle Commerzbank)

Begriffe (4/5)

- **Beweis / Beweismittel**

- Der Beweis ist das Mittel, um das Gericht im Prozess von einer bestrittenen Tatsache zu überzeugen. Er wird nur über Tatsachen erhoben. (Quelle www.juraforum.de)
- Beweismittel sollen die Überzeugung des Richters über eine Tatsache herbeiführen. (Quelle www.juraforum.de)

Begriffe (5/5)

- **IT-Forensik:**

- Vorfälle im Sinne der IT Forensik sind tatsächliche oder vermutete Ereignisse, die schadhafte oder gefährdende Auswirkungen auf IT-Systeme des Commerzbank Konzerns haben. IT Forensik rekonstruiert den zur Analyse vorliegenden Sachverhalt auf Basis von Tatsachen mit dem Ziel der Sondierung des potenziellen bzw. tatsächlichen Schadens sowie des verbleibenden Risikos. (Quelle Commerzbank)

- **Incident Response:**

- Unter den Begriff „Incident Response“ (...) fallen alle Aufgaben und Funktionen, die mit der Reaktion auf Vorfälle in einem konkreten technischen oder organisatorischen Zusammenhang stehen. (Quelle www.dfn-cert.de)

Overview / Agenda

1. Definition Begrifflichkeiten
2. Rollen und Verantwortlichkeiten
3. Der IT-forensische Prozeß
4. Organisation und Vorbereitung einer IT-forensischen Untersuchung
5. Durchführung einer IT-forensischen Untersuchung
6. Abschluß und Nachbereitung einer IT-forensischen Untersuchung

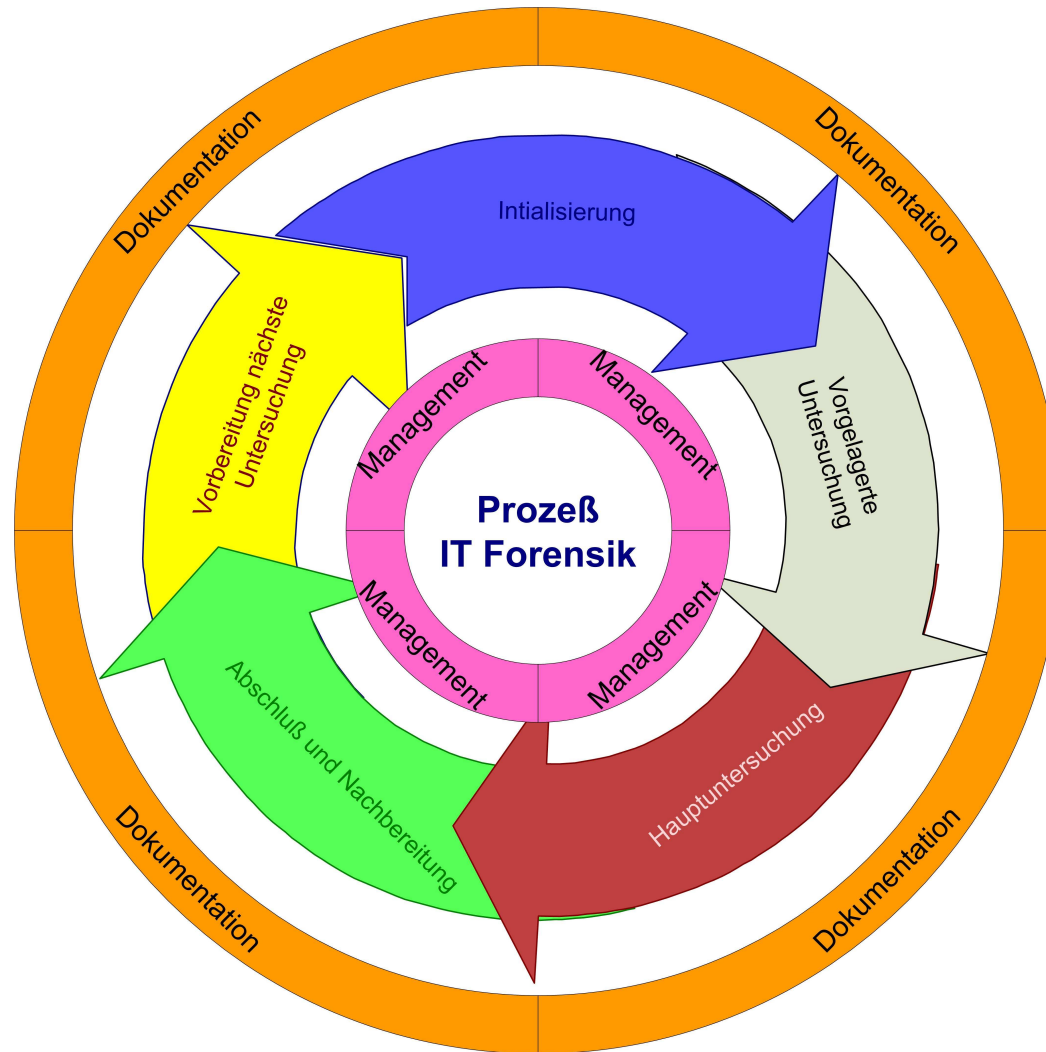
Rollen und Verantwortlichkeiten

- Leiter der Untersuchung
- Spezialisten für
 - IT Forensik
 - Recht
 - Kommunikation
 - Personal
 - Compliance
 - Geschäftsprozeß/Fachabteilung
- Revision
- Management

Overview / Agenda

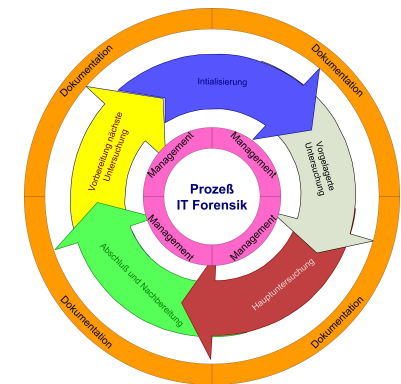
1. Definition Begrifflichkeiten
2. Rollen und Verantwortlichkeiten
3. **Der IT-forensische Prozeß**
4. Organisation und Vorbereitung einer IT-forensischen Untersuchung
5. Durchführung einer IT-forensischen Untersuchung
6. Abschluß und Nachbereitung einer IT-forensischen Untersuchung

Der IT-forensische Prozess im Überblick



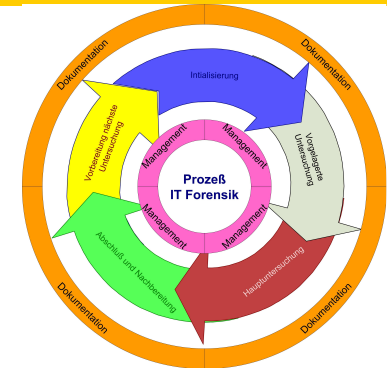
Management

- Sobald die Meldung über einen Vorfall eingeht, müssen die Verantwortlichkeiten gemäß definierten Rollen installiert werden
- Sowohl der Prozess wie auch die einzelnen Phasen müssen konsequent gesteuert und kontrolliert werden
- Die Kommunikation, insbesondere gegenüber dem Top-Management ist eine vorrangige und erfolgskritische Führungsaufgabe



Dokumentation

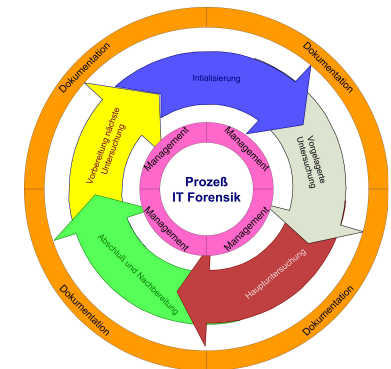
- Grundsätzlich sollte eine schriftliche Vorgabe zur IT-Forensik im Unternehmen existieren!
- Wenn die Meldung über einen Vorfall eingeht, so sind folgende Schritte durchzuführen:
 - Dokumentation wann und von wem der Vorfall gemeldet wurde,
 - Beschreibung des Vorfalls,
 - Dokumentation der vermuteten Auswirkungen,
 - Grobplanung der nächsten Schritte (schriftliche Kurznotiz)
 - Aktivierung des IT Forensik Teams (schriftliche Anweisung)
- Während der Durchführung der forensischen Analysen ist eine kontinuierliche Dokumentation unerlässlich



Initialisierung des Prozesses (1/2)

Wer kann eine forensische Untersuchung initiieren?

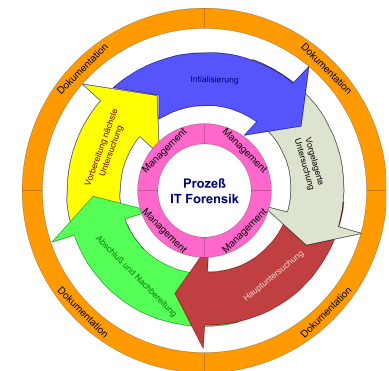
- Über die definierten Meldewege jeder Mitarbeiter des Unternehmens
- Das Management aufgrund seiner Kompetenz
- Die Fachabteilungen aufgrund besonderer Vorkommnisse im Geschäftsbetrieb
- Die IT-Abteilungen als Verantwortliche für Entwicklung und Betrieb der IT-Systeme
- Die Abteilungen mit hoheitlichen Aufgaben aufgrund besonderer Umstände



Initialisierung des Prozesses (2/2)

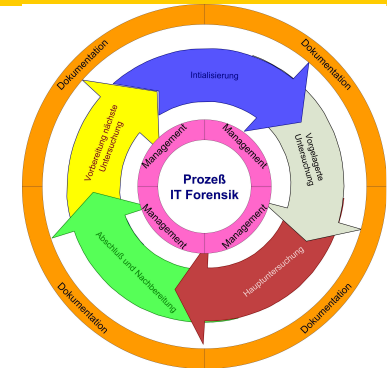
Warum wird eine forensische Untersuchung angefordert?

- Bedienen der Unternehmensanforderung (Nachvollziehbarkeit): Technische und inhaltliche Aufklärung eines intransparenten Sachverhaltes bzw. Vorgangs
- Bedienen der juristischen Aspekte
 - Individualsicht (Unternehmen vs. Verursacher)
 - Arbeitsrechtliche Ebene
 - Zivilrechtliche Ansprüche
 - Strafrechtliche Konsequenzen
 - Regulatorische Sicht (Unternehmen vs. Staat)
 - Nationale und internationale Aufsichtsbehörden (compliance)



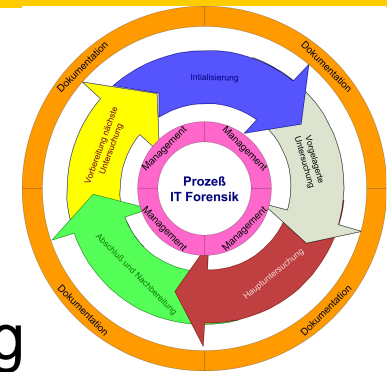
Vorbereitung der vorgelagerten Analyse

- Inhaltliche Aspekte („roter Faden“)
 - Erste Festlegung der Vorgehensweise
 - Grobdefinition zu untersuchender Parameter
 - Grobe Risikoabschätzung
- Finanzielle Aspekte (Initiale Abschätzung des benötigten Budgets)
- Organisatorische Aspekte
- Vorbereitung der Dokumentationsstruktur



Hauptuntersuchung

- Informationssammlung/Beweisaufnahme
- Informations-/Beweisbewertung und Timelining
- Informationsaufbereitung
- Präsentation der Ergebnisse



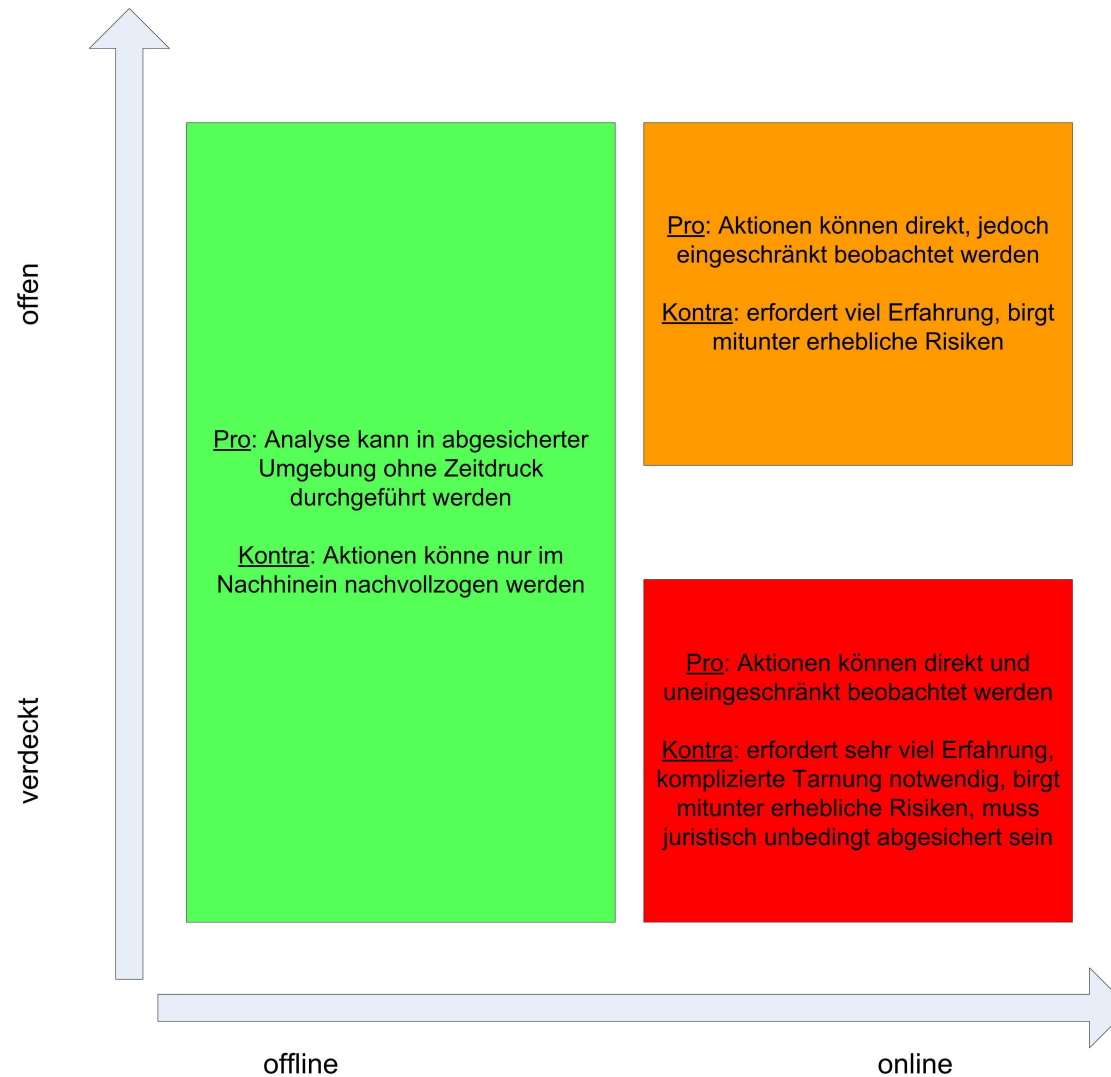
Overview / Agenda

1. Definition Begrifflichkeiten
2. Der IT-forensische Prozeß
3. Rollen und Verantwortlichkeiten
4. Organisation und Vorbereitung einer IT-forensischen Untersuchung
5. Durchführung einer IT-forensischen Untersuchung
6. Abschluß und Nachbereitung einer IT-forensischen Untersuchung

Organisation und Vorbereitung

- Zusammenstellung und Aktivierung des Forensic Teams
- Definition der standardisierten Vorgehensweise für die Informationssammlung (SOP)
 - online/offline
 - verdeckt/offen
- Definition der IT-Ausstattung für die Informationssammlung
- Definition des forensischen Arbeitsplatz für die Informationsauswertung
- Bereitstellung von Räumlichkeiten für das Forensic Team
- Verfügbarkeit von Budget (Reise, externe Unterstützung, Spezial HW/SW) oder dessen kurzfristige Beschaffbarkeit

Informationssammlung: Alternativen



Overview / Agenda

1. Definition Begrifflichkeiten
2. Der IT-forensische Prozeß
3. Rollen und Verantwortlichkeiten
4. Organisation und Vorbereitung einer IT-forensischen Untersuchung
5. Durchführung einer IT-forensischen Untersuchung
6. Abschluß und Nachbereitung einer IT-forensischen Untersuchung

Beweisaufnahme => Grundsätzliches

- Dokumentation aller Aktivitäten
- Anwendung des Vier-Augen-Prinzips
- Unbedingte Beachtung der Prinzipien zur Erhebung von Beweismitteln
- Ohne eine formale, anwendbare Methodik entbehrt eine Untersuchung jeder wissenschaftlichen Grundlage. Eine solche „hemdsärmelige“ Ad-hoc Vorgehensweise wird vor Gericht als komplett unseriös zurückgewiesen, da sie keinerlei Aussagekraft besitzt.

Grundregeln zur Suche und Erhebung von Beweismitteln (1/2)

- Beweismittel dürfen unter keinen Umständen verändert werden
- Es dürfen keine Programme auf IT-Systemen am Tatort bzw. denjenigen, die mit dem Tatort in Zusammenhang stehen, ausgeführt werden
- Potentiell verdächtige Personen dürfen nicht auf IT-Systemen am Tatort bzw. denjenigen, die mit dem Tatort in Zusammenhang stehen, Tätigkeiten durch- bzw. Aktionen ausführen

Grundregeln zur Suche und Erhebung von Beweismitteln (2/2)

- Alle relevanten IT-Systeme am Tatort bzw. diejenigen, die mit dem Tatort in Zusammenhang stehen müssen bitgleich kopiert werden. Bei IT-Systemen, die noch live sind, sollte nach Möglichkeit alle flüchtigen Informationen vor dem Ausschalten gesichert werden
- Alle Aktivitäten der Untersuchung sind detailliert zu dokumentieren
- Bei allen Formen der Beweismittelerhebung ist derjenige Ansatz zu wählen, der am wenigsten invasiv ist, um Verfälschungen oder Zerstörung des Beweismittels zu vermeiden

Schritte der Beweismittelerhebung

- Plan bzw. Vorgehensweise zur Beweismittelerhebung formulieren,
- Tatort aufsuchen, betreten und sichern,
- Tatort dokumentieren,
- Beweismittel suchen,
- Beweismittel erheben,
- gegebenenfalls Untersuchung des Live-Systems (nur wenn unbedingt notwendig!) [Beweismittel extrahieren]

Beweismittel suchen (1/x)

- Jeder Fall, unabhängig wie vermeintlich einfach dieser auch auf den ersten Blick ist, sollte strikt nach der vereinbarten Methodik abgearbeitet werden.
- Die Suche nach primären technischen Beweismitteln wird durch die technischen Analysten durchgeführt. Die spezifische Taktik wird durch sie bestimmt und hängt insbesondere von den Rahmenbedingungen ab
- Die Suche nach nicht-technischen Kontextinformationen sollte nach einem durchgängigen Prinzip erfolgen. Grundlage hierfür ist die räumliche Gliederung des Tatortes (z.B. in Quadranten, Streifen, Spiralen)

Beweismittel suchen (2/x)

- Der Erfahrung nach sind folgende Orte ergiebige Quellen für nicht-technische Kontextinformationen
 - Desktop: post-it, Datenträger, Handbücher, Computerzubehör, Kabel
 - Bildschirm: post-it Notizen mit Passwörtern oder anderen wichtigen Informationen
 - Telefon und Umgebung: Benutzernamen, Passwörter, Notizen, Nummern
 - Mülleimer: alle Sorten von mitunter wichtigen Informationen
 - Tastatur: Notizen, Passwörter, Disketten, sonstige Informationen
 - Fachbücher/Handbücher: Notizen aller Art, Datenträger
 - Büroumgebung: Hinweise auf Passwörter (Hobbys, Familie, etc.)

Beweisbewertung

- Erstellung einer Arbeitskopie von der Masterkopie
- Timelining (timeskew, Referenzzeit festlegen).
- Strukturierung der Detailuntersuchungen gemäß der festgelegten Ermittlungsziele
- Bewußtmachung der besonderen Rahmenbedingungen
- Gliederung nach Untersuchungsschwerpunkten

Beweisbewertung => Strukturierung der Detailuntersuchungen

- Welche Untersuchungsmethode führt dazu, dass ich die gewünschten Ziele bestätigen bzw. widerlegen kann?
- Welche Untersuchungen müssen noch durchgeführt werden, welche sind bereits abgeschlossen?
- Wurden bereits verwertbare Ergebnisse (be- sowie entlastend ermittelt?
- Haben sich Ergebnistypen im Laufe der Untersuchungen verändert?

Beweisbewertung => Bewußtmachung der besonderen Rahmenbedingungen

- "Manchmal sind Dinge gar nicht so komplex wie angenommen", d.h. Verdächtige sind einfältig!
- "Ergebnisse sind nicht immer offensichtlich", z.B. Filesystem hinter Filesystem
- "Vermeintlicher Datenmüll ist nicht immer ein solcher", z.B. Manipulation der MFT
- "der offensichtliche Inhalt eines files ist nicht immer der tatsächliche", z.B. Steganographie

Informationsaufbereitung/Ergebnisdarstellung

- Darstellung von Fakten
- Abgrenzung von Interpretationen

Präsentation der Ergebnisse

- Art der Präsentation
- "keep it straight, keep it simple"
- "ein Bild sagt mehr als tausend Worte"
- fachliche Beurteiler verfügen in der Regel über kein technisches Wissen!

Overview / Agenda

1. Definition Begrifflichkeiten
2. Der IT-forensische Prozeß
3. Rollen und Verantwortlichkeiten
4. Organisation und Vorbereitung einer IT-forensischen Untersuchung
5. Durchführung einer IT-forensischen Untersuchung
6. Abschluß und Nachbereitung einer IT-forensischen Untersuchung

Abschluß der Untersuchung und Nachbereitung

- Zum Abschluss ist ein umfangreicher Untersuchungsbericht als Zusammenfassung der Akte zu erstellen.
- Durchführung von lessons learned
- Prüfung, ob es Auswirkungen auf die entsprechenden Unternehmensvorgaben, die relevanten Prozesse oder die spezifischen Vorgehensweisen gibt

Vorbereitung der nächsten Untersuchung

Frei nach Josef „Sepp“ Herberger:

- Nach der Untersuchung ist vor der Untersuchung,
- Allerdings dauert eine Untersuchung leider nicht 90 Minuten,
- Meistens ist auch nur der Ball rund, denn die Erfahrung zeigt, dass jede Untersuchung Unwägbarkeiten bereithält und
- Der nächste Gegner ist immer der schwerste!

Fazit: Man macht es so wie immer, nur halt eben jedes Mal etwas besser!

***For most of the cases there is a solution, but
leave it to the experts!***



Quelle:
Birgitt Bolsmann
„Im Labyrinth“
1982, Eitempera und Öl auf
Leinwand, 75 x 75 cm

Noch Fragen?



**Vielen Dank für Ihre
Aufmerksamkeit!**

Kontakt:

Dr. Igor Podebrad

Head of Threat Analysis & Forensic

- 069-136-40630
- igor.podebrad@commerzbank.com

Commerzbank AG