IT-Forensik im betrieblichen Umfeld

Aachen, 17. Mai 2011

Dr. Rainer Thomas

GENERALI Informatik Services

IT-Forensik im betrieblichen Umfeld

Notwendigkeit zur IT-Forensik?

Notwendigkeit besteht indirekt – um handlungsfähig zu sein

Anforderungen:

- BAFin MA Risk VA
  - Risikomanagement (Bewertung von Risiken)
  - Notfall-Management (BCM)
- ISO 27001/2 A13 (Standard für Informationssicherheitsmanagementsysteme)
- ISO 27035 (zukünftig)
- BDSG (z.B: §42a)
- Nachweis der Ordnungsmäßigkeit (z.B. Zertifizierung nach PS 951)

IT-Forensik im betrieblichen Umfeld

Kann man IT-Forensik / Security Incident Management outsourcen?

Wie häufig muss man aktiv werden? → Selten
Trotzdem ist es wichtig, für forensische Untersuchungen vorbereitet zu sein.

Warum selber machen?

- Kenntnis des Konzerns, der Technik, der Personen und der Rollen (auch für Unterstützung von externen Ermittlern)
- Unübersichtliche Systemlandschaft – das Know How bei konkreten Systemen liegt verteilt bei den CCs / Betriebsexperten
- Die technischen Anforderungen sind häufig eher niedrig
- Minimierung der Reaktionszeit
- Weniger Bewegungen der Beweismittel
- Vertraulichkeit (intern <-> extern)
- Konsequenzen für Mitarbeiter: Arbeitsrecht, u.U. Zivilrecht
- Am Anfang weiß man nicht, was am Ende herauskommt
  → Von Anfang an so vorgehen, dass man für alles gewappnet ist

Externe Schnittstellen

- Fallback technisch: externer DL (Kompetenz, Erfahrung, Spezialtechnik (z.B. Kroll Ontrack))
- Zusammenarbeit mit Behörden, z.B. wenn Strafrecht betroffen ist (Polizei, …)

IT-Forensik im betrieblichen Umfeld
Priorität

Priorität = hoch!

- Auswirkungen können weitreichend sein
- Interne Aufmerksamkeit
- Ggf. Außenwirkung (Image, Presse, Behörden, …)

IT-Forensik im betrieblichen Umfeld

Ziele der IT-Forensik (und des Security Incident Managements)

Neben den inhaltlichen sind auch die organisatorischen Anforderungen zu erfüllen

Inhaltlich

- Feststellen von wer, wie, was, ...
- Erstellen von Analyseberichten, Einleiten von Maßnahmen, …

Organisatorisch

- Erfüllen innerer und äußerer Anforderungen (verschiedene Anspruchsgruppen)
- Wahren des organisatorisch ordnungsmäßigen Ablaufs (Einhaltung der Rollen)
- Schutz des Unternehmens, der Mitarbeiter und der Daten
- Schutz der Mitarbeiter vor ordnungswidrigem Verhalten (z.B. bei äußerem Druck)
- Schutz der Mitarbeiter vor falschen Anschuldigungen

IT-Forensik im betrieblichen Umfeld
Einordnung in die Prozesslandschaft

IT-Forensik ist eine Komponente des Security Incident Managements

Schnittstellen:

- Definierte Meldewege (Meldepflicht für Sicherheitsvorfälle!)
  - UHD, Incident Management, Problem Management, ..
  - Dokumente, Anweisungen
- Eskalation nach / Information von:
  - Notfallvorsorge / Business Continuity Management / Krisenmanagement
  - Revision, Personalabteilung, Rechtsabteilung, …

IT-Forensik im betrieblichen Umfeld
Rollentrennung

Verschiedene Aufgaben <-> Jeder handelt in dem für ihn zulässigen Rahmen!

Relevante interne Rollen
- Revision
- Personalabteilung
- Konzernunternehmen (i.d.R. Eigentümer der Daten)
- Datenschutz
- Betriebsrat
    - Betriebsvereinbarungen
- Rechtsabteilung
- IT-Sicherheit

IT-Forensik im betrieblichen Umfeld
Der Ermittlungsauftrag

Bedingt durch die verschiedenen Rollen ist eine Beauftragung notwendig!
Es finden keine systematischen Untersuchungen statt. Ermittlung nur mit Auftrag!

Beispiel:
Ein Unternehmen will feststellen, ob ein Mitarbeiter sich mit der Benutzerkennung eines Kollegen angemeldet hat. Auf die Anmeldedaten hat aber nur der IT-Dienstleister Zugriff.

- Das Unternehmen ist Eigentümer der Daten und will den Vorfall klären.
- Der IT-Dienstleister hat das Know-How und den technischen Zugriff.

→ Das Unternehmen beauftragt den IT-Dienstleister, auf dem Client, dem Domänenserver und in der Maildatenbank nach Anmeldedaten und einer verschickten Email zu suchen

Wichtige Komponenten im Ablauf:
- Auftrag mit angemessener Beschreibung der durchzuführenden Aktivitäten (nach Beratung und Abstimmung)
- Prüfen der Zulässigkeit beim IT-Dienstleister (Sind Gremien ausreichend einbezogen? Passt die Untersuchung zum Vorwurf? Ist der Umfang der zu ermittelnden und zu liefernden Daten angemessen und rechtlich zulässig? ….)
- Eigene Durchführung / Interne Beauftragung der operativen Tätigkeiten (z.B. an Notes-Admins)
- Zusammenstellen und Prüfen der Daten / Erstellen eines Berichts / Übergabe an Auftraggeber

IT-Forensik im betrieblichen Umfeld

Ordnungsmäßiges Vorgehen

Ordnungsmäßigkeit muß gewährleistet sein

Wichtige Aspekte bei der Durchführung der Ermittlung

- 4-Augen Prinzip (QS, Dokumentation, …)
- Unabhängigkeit und Objektivität (belastendes und entlastendes)
- Umfassende Dokumentation (Formulare / Protokolle)
  - Erlangung von Beweismitteln
  - Beweismittelprotokoll
  - Analyse-Protokoll
  - Verwahrung von Beweismitteln (abschließbarer Raum, Schrank)
  - Sichere Lagerung und Übertragung von Daten
- Korrektes Einbeziehen von internen DL
  - Admins
  - Systemexperten
- Einhalten von Gesetzen (TKG, Persönlichkeitsrecht, StGB 202, 203, …)

IT-Forensik im betrieblichen Umfeld
Technische Fragestellungen

Wesentliche Anforderung an die vorhandene Analysetechnik:
→ aktueller Gerätebestand muss abgedeckt sein

Beispiele:
- Auswertungsrechner (Stand-alone oder am Firmennetz?)
- Xways Forensics
- Write-Blocker (Tableau)
- Adapter, DVD Brenner, Externe Platten
- Sonstige Hilfsmittel (Tüten, Tacker, Fotoapparat, …)

Medien:
- Festplatten, Sticks (Verschlüsselung vorhanden?)
- Netzlaufwerke, Maildatenbanken

Üben:
- Bei neuen Notebooks: Platten finden und ausbauen

Technisch unwegsames:
- Hostplatten, RAID, Kassettenroboter, …

IT-Forensik im betrieblichen Umfeld
Fälle in der Praxis

Keine Verfolgung von Bagatellfällen!

Meist IT-mäßige „Trivialfälle“
- Nichtdienstliche Nutzung
- Betrug

Selten:
- „Schwere“ Gesetzesverstösse
- Virenvorfälle
- Identitätsdiebstahl
- Erfolgreiche Hackerangriffe
- „Hochverrat“

Mögliche Beispiele:
- Mitarbeiter bringt Notebook mit in die Firma und klemmt ihn ans Netz. Auf dem Rechner ist ein Trojaner.
- Außendienst-Mitarbeiter kündigt und gibt den von der Firma gestellten Rechner nicht zurück.
- Im Foyer gefundener USB-Stick.
- Bei einer Prüfung festgestellte Firewallregel, mit der ein Client ohne Filterung in das Internet kommt.
- Ein abends heruntergefahrener PC ist morgens an.
- Die Maus eines Mitarbeiters bewegt sich ohne sein Zutun.

IT-Forensik im betrieblichen Umfeld
Rahmenbedingungen

Die Rahmenbedingungen sind häufig Forensik-behindernd

Prioritäten der IT-Forensik im Betrieb, SIM vs. IM
→ Verfügbarkeit ist wichtigstes Ziel
- Clients werden schnell neu aufgesetzt
- Eingriffe in Betrieb abhängig von der Kritikalität
- Zentrale Systeme stoppen ist fast nicht möglich

Nur existierende Daten sind auswertbar
- z.B. Existenz und Aufbewahrungsdauer von Logs
- Die Generierung von Logs / Monitoring / Alerting wird bei der Systemerstellung für die Betriebssicherheit ausgelegt. Nicht für die Verwendung bei forensischen Maßnahmen.

Schwierigkeiten in der Kommunikation
- Was ist wichtig oder unwichtig? → spät und plötzlich auftauchende wichtige Infos
- Selektive Information zwischen den Beteiligten
- Das „Stille Post“ – Phänomen: sich verändernder Inhalt beim Weiterleiten von Infos
- Unterschiedliches Know-How der Beteiligten (Übersetzungsproblematik)

Verfolgung von Vorfällen nach außen sinnvoll? → Ist fallweise zu prüfen.

IT-Forensik im betrieblichen Umfeld
Auswertung von Vorfällen

Jeder Fall wird ausgewertet!

Auswertung von Vorfällen zu folgenden Zwecken
- Statistik
  - Aufwand
  - Trends
- Know How Aufbau
  - zusätzlich benötigtes Gerät
  - Bedarf an Schulungen
- Interner Ablauf
  - Einhaltung und Schärfung der internen Rollen

Auswirkungen auf die Risikosituation
- Ist der Vorfall durch ein bestehendes Risiko begünstigt worden
- Ist durch den Vorfall ein Risiko entstanden?
- Ggf. Meldung an das Risikomanagement

Vielen Dank für Ihre Aufmerksamkeit!