it.sec
security for your information

Herausforderungen bei der IT-Forensik im Kontext outgesourcter IT

Workshop der GI-FGs SECMGT, FoMSESS & EZQN
sowie des DIN NA 043-01-27-04 (AK 4) am 14.06.2013

Bernhard C. Witt (it.sec GmbH & Co. KG)

Bernhard C. Witt

- Senior Consultant für Datenschutz und Informations-sicherheit bei der it.sec GmbH & Co. KG verantwortlich für die Geschäftsfelder
  ° Datenschutz (→ externer Datenschutzbeauftragter)
  ° IT Governance, Risk & Compliance Management
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- zertifizierter ISO/IEC 27001 Lead Auditor (BSi)
- CRISC (ISACA)
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor der Bücher „IT-Sicherheit kompakt und verständ-lich“ (2006) und „Datenschutz kompakt und verständlich“ (2008 & 2010)
- Sprecher der GI-Fachgruppe Management von Infor-mationssicherheit (seit 2009)
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit (seit 2009)
- Mitglied im Leitungsgremium der GI-Fachgruppe Datenschutzfördernde Technik (seit 2012)
- Mitglied im DIN-Arbeitsausschuss „IT-Sicherheitsverfah-ren“ AK 1 & 4 (seit 2011)

it.sec
security for your information

Zur it.sec GmbH & Co. KG

IT Governance, Risk & Compliance Management

- Management von Informations-sicherheit & Business Continuity
- Toolgestütztes IT Governance, Risk & Compliance Management
- Compliance zu multiregulatorischen Anforderungen (inkl. internationaler Standards)
- Sicherheitskonzepte, Policies, Prozesse & Prozeduren

Penetrationstests, IT-Forensik Assessments & Audits

- Penetrationstests IT-Infrastruktur & Web-Applikations-Sicherheit
- IT Security & Compliance Checks
- Abwehr von Targetted / Client-side Attacks
- Beweissicherung, IT-Forensik & eDiscovery

Infrastruktursicherheit & Data Protection

- Härtung Server-, Client- & Netzwerk-systeme
- Intrusion Detection & Prevention
- Data Leakage Detection & Prevention
- SCADA Security

Datenschutz

- Externer Datenschutzbeauftragter
- Datenschutzaudits & Auftrags-kontrollen
- Datenschutzkonzepte
- Schulungen

Zur GI-FG SECMGT

Die GI-Fachgruppe **Management von Informationssicherheit**

bietet den im Bereich des Managements von Informationssicherheit tätigen Personen eine neutrale Plattform, um sich miteinander zu vernetzen sowie Wissen und Erfahrungen auszutauschen.

- ist Teil der **Gesellschaft für Informatik** e.V. (gemeinnützige Fachgesellschaft zur Förderung der Informatik)
- beschäftigt sich mit der Verzahnung von informationstechnischen sowie organisatorischen Schutzmaßnahmen und dem Risikomanagement in Behörden oder Unternehmen
- vertritt praxisorientierte Themen zu Management, Konzeption, Betrieb und Fortentwicklung von Informationssicherheit
- veranstaltet mehrere Workshops pro Jahr (auch Nichtmitglieder sind stets willkommen); durch Teilnahme können CPEs erworben werden
- hat AK zu kritischen Informations- & Kommunikationsinfrastrukturen

→ **Nähere Informationen unter www.fg-secmgt.gi.de**

IT-Forensik (1)

Was versteht man unter IT-Forensik?

- IT-Forensik ist als streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen anzusehen [gem. BSI-Leitfaden „IT-Forensik“, Stand 2011]
  → klare Definition zur Methodik wichtig
  → wohldefinierte Methodik ist konsequent anzuwenden
  → **Ziel** der IT-Forensik ist die Datenanalyse zur Aufklärung von Vorfällen
  → beantwortet also: WAS hat WER WANN (WARUM) WIE WO gemacht?
- **ISO/IEC 27037: digital evidence**
  information or data, stored or transmitted in binary form that may be relied on as evidence
- **ISO/IEC 13888-1: evidence**
  information which is used, either by itself or in conjunction with other information, to establish proof about an event or action

IT-Forensik (2)

Standardisierungsvorhaben mit Bezug zur IT-Forensik:

- **ISO/IEC 27035**: Information Security Incident Management
- **ISO/IEC 27037**: Leitfaden zur Erzeugung digitaler Evidenz
- **ISO/IEC 27038**: Vorgehen zur beschränkten Datenoffenbarung
- **ISO/IEC 27040**: Sichere Datenhaltung
- **ISO/IEC 27041**: Anleitung für die Auswahl geeigneter Untersuchungsmethoden
- **ISO/IEC 27042**: Leitfaden zur Analyse und Interpretation digitaler Evidenz
- **ISO/IEC 27043**: Prinzipien und Prozesse zur Untersuchung von Vorfällen und zu den gebotenen Voraussetzungen
- **ISO/IEC 27044**: Leitfaden zum Security Information & Event Management
- **ISO/IEC 27050**: Vorgehen im Rahmen von eDiscovery-Verfahren
- **ISO/IEC 30121**: Steuerung digitaler Forensik-Risiken

Outsourcing von IT-Services (1)

Welche Herausforderungen sind zu beachten,

wenn IT-Services durch externe Stellen erbracht werden?

- Beim Outsourcing gibt es grundsätzlich zwei verschiedene Modelle:
  - ° **Auftragsdatenverarbeitung**: Auftraggeber bleibt weisungsbefugt
    → Vollständige Steuerung durch Auftraggeber
  - ° **Funktionsübertragung**: Auftragnehmer übernimmt die Funktion
    → Auftraggeber erhält nur Dienstleistung / Werk / Mietobjekt
- **Besonderheit im Datenschutzrecht**:
  - ° Auftragsdatenverarbeitung präzise definiert in § 11 BDSG
    → Verstoß bußgeldbewährt (§ 43 Abs. 1 Nr. 2b BDSG)
  - ° Funktionsübertragung liegt vor, wenn Anforderungen aus § 11 BDSG nicht vollständig erfüllt sind
    → Datenempfänger an Zweck der Datenerhebung & -speicherung gebunden (§ 28 Abs. 5 BDSG), sofern keine Zweckänderung unter Vornahme einer Abwägung nach § 28 Abs. 2 BDSG durchgeführt wurde und die Übermittlung hier noch zulässig ist (zulässiges Senden und zulässiges Empfangen)

Outsourcing von IT-Services (2)

Herausforderungen beim Outsourcing:

- Auftragnehmer hat u.U. **anderen Risikoappetit** als ihre Auftraggeber (Pönale i.d.R. weit geringer als potenzieller Schaden bei Eintritt des Risikos!)
- Auftragnehmer verwendet oft **andere Risikoanalyse Methodologie** als ihre Auftraggeber (gemäß dem gewählten Geschäftsmodell!)
- Auftragnehmer hat **andere Vorstellung hinsichtlich meldepflichtiger Security Incidents** als Auftraggeber, wenn dies nicht ausdrücklich festgelegt wurde (ist aber nur bedingt möglich)
- Für Auftragnehmer ist es i.d.R. von **nachrangigem Interesse**, **welche Datenkategorien** im Auftrag verarbeitet werden, für Auftraggeber sind dagegen die überlassenen Daten u.U. grundlegend

→ jeweilige Informationssicherheitsmanagementsysteme (ISMS) oft sogar stark voneinander abweichend!

→ **Hilfestellung durch Standardisierung insoweit sehr willkommen**

Outsourcing von IT-Services (3)

Bisherige Hilfestellungen durch Standardisierung:

- **ISO/IEC 24762**: Gewährleistung ausreichender Disaster Recovery im Kontext von Outsourcing
  → Schutz der Datenbestände des Auftraggebers
- **ISO/IEC 27036-x**: Informationssicherheit in der gesamten Supply Chain der verwendeten Informations- & Kommunikationstechnik
  → Acquirer und Supplier haben auszuhandeln:
  1. Welche Informationen über Sicherheitsniveau sind nötig?
  2. Welche Kontrollrechte sind für Acquirer erforderlich?
  3. Ab wann besteht ein ausreichendes Vertrauen?
- **ISO/IEC 20000-x**: Zertifizierung von IT-Services (mit Bezug zu ITIL)

Cloud Services

Welche zusätzlichen Aspekte greifen,

wenn IT-Services in der Cloud erbracht werden?

- Bei Cloud Services hat der Auftraggeber keinen Einfluss auf die Auftragserledigung (hinsichtlich Art und Ort). Er kann einen angebotenen Service lediglich annehmen oder ablehnen.
  → Vertrauensstellung durch unabhängige Kontrolle Dritter
  → Nachvollziehbarkeit durch definierte Service Level Agreements
  → Beurteilung der Eignung des Services anhand der Zusagen des Cloud Providers
- Standardisierung kann helfen, dass es hier vergleichbare Mindeststandards gibt, die, sofern sich der Cloud Provider daran hält, dem Nutzer in ausreichender Weise versichern, dass ein angemessenes Sicherheitsniveau beim Cloud Provider eingehalten wird.
  → **ISO/IEC 27017**: Informationssicherheit von Cloud Services
  → **ISO/IEC 27018**: Datenschutz bei Cloud Services
  → **ISO/IEC 27036-4**: Leitfaden zur Informationssicherheit von Cloud Services

Probleme bei IT-Forensik outgesourcter IT (1)

Welche Probleme sind zu lösen, wenn aufgrund eines Security Incidents bei outgesourcter IT IT-forensische Untersuchungen angestellt werden sollen?

- Mit dem Auftragnehmer sollten Regelungen zur **Beweissicherung** vereinbart werden
  - → Zeitpunkt für den Beginn der Beweissicherung festlegen (Meldung bzw. Feststellung des Security Incidents)
  - → Vorgehen zur Beweissicherung vereinbaren (Stand bei Eintritt des Security Incidents, Behebungsmaßnahmen & Stand nach Durchführung der Behebungsmaßnahmen dokumentieren)
  - → Bereitstellung der Beweissicherungsdaten für Auftraggeber & Staatsanwaltschaft regeln
  - → **allgemein anerkannte ISO/IEC-Standards hilfreich**!
- Nichteinhaltung der Vereinbarung zur Beweissicherung sollte empfindliche Pönale auslösen (aber: Auftragnehmer wird z.T. die Zahlung einer Pönale der korrekten Abarbeitung vorziehen!)

Probleme bei IT-Forensik outgesourcter IT (2)

- Bei Einsatz von **Shared Services** treten zusätzliche Probleme auf:
  - ° Beweissicherungsverfahren tangieren u.U. **Daten anderer Nutzer**
    - → Beachtung der datenschutzrechtlichen Datentrennung
    - → ggf. Bereinigung der Datensätze (Ausfilterung der Daten anderer Nutzer)
  - ° Beweissicherungsdaten offenbaren u.U. geschützte **Betriebs- und Geschäftsgeheimnisse** über Einstellungen, Skripte, Umsetzung technischer Prozesse
    - → Zweckbindung auch in anderer Richtung vereinbaren
    - → unabhängige IT-forensische Untersuchung durchführen
  - ° **Nichtbereitstellung** erforderlicher Beweissicherungsdaten führt i.d.R. sogar recht oft zum vorzeitigen Ermittlungsende bei zivilrechtlichen Verfahren
    - → Ausdrückliche Regelung für sicherheitsrelevante Fälle treffen
    - → ggf. Einsatz eines Datentreuhänders
  - → **auch hier könnten allgemein anerkannte ISO/IEC-Standards helfen**!

Ergänzende Literatur mit Praxisbezug

- Bernhard C. Witt: CSI Cyberspace – Anforderungen an die Durchführung IT-forensischer Untersuchungen, <kes> 2011#3, S. 51 – 56.
- Bernhard C. Witt: Im Auftrag des Herrn – Theorie und Praxis der Auftragsdatenverarbeitung, <kes> 2012#2, S. 6 – 10.
- Holger Heimann: Der schöne Schein – Was Sicherheitszertifikate von Dienstleistern aussagen – und was nicht, <kes> 2013#2, S. 6 – 9.

Vielen Dank für Ihre Aufmerksamkeit!

it.sec GmbH & Co. KG
Einsteinstr. 55
D-89077 Ulm

USt Id Nr.: DE 225547544
Steuernummer: 88012/53709
Amtsgericht Ulm: HRA 3129

vertreten durch den **Geschäftsführer Dipl. Ing. (FH) Holger Heimann**

Haftender Komplementär:
it.sec Verwaltungs GmbH
Amtsgericht Ulm: HRB 4593
Einsteinstr. 55
D-89077 Ulm