SCOPAR

S-ITsec: strategisches IT-Security-Managementsystem

IT-Sicherheit: Risiken erkennen, bewerten und behandeln

„…Ein etabliertes IT-Security-Managementsystem (ISMS) ist ein kritischer Erfolgsfaktor für ein Unternehmen. Wichtig ist, die Sicherheit an den realen Bedrohungen auszurichten, um nicht „mit Kanonen auf Spatzen zu schießen…“

Gerhard Funk
Dipl.-Ing., CISA, CISM
Mitglied des SCOPAR-Beratergremiums

MIT BLICK FÜRS GANZE ..

Inhalt

IT-Risiken – einige Beispiele: Hackerangriffe und verlorener Laptop

kleiner Auszug erfolgreicher Hackerangriffe Januar und Februar 2013:

- Renault Argentinien: Adressdaten von über 37T Kunden wurden veröffentlicht.
- WWF China: Adressdaten von rund 80T Personen wurden veröffentlicht.

Quellen: searchsecurity.de, hackmageddon.com

Bitkom und ENISA warnen vor Cybercrime
Die zehn größten Gefahren im Internet
Platz 1: Drive-by-Downloads von Schadsoftware
Platz 2: Trojaner / Würmer
Platz 3: Attacken auf Datenbanken und Websites
…
Quelle:
http://www.searchsecurity.de/themenbereiche/bedrohungen/phishing-und-spam/articles/393304/

The Cost of a Lost Laptop

Sponsored by
Intel Corporation
Independently conducted by Ponemon Institute LLC
Publication: April 22, 2009

Ponemon Institute©

Table 1: Seven cost component	Average cost
Laptop replacement cost	1,582
Detection & escalation cost	262
Forensics & investigation cost	814
Data breach cost	39,297
Intellectual property loss	5,871
Lost productivity cost	243
Other legal or regulatory costs	1,177
Total	$49,246

Datenschutz:
Wenn verlorene Laptops Millionen kosten
http://www.crn.de/security/artikel-95221.html

Ist das Entwickeln sicherer Software Geldverschwendung?
Zitat: „ … es immer noch keinen Konsens gebe, wie man letztendlich zu sicherer Software komme.“
Quelle: http://www.heise.de/security/meldung/Ist-das-Entwickeln-sicherer-Software-Geldverschwendung-1813564.html

Ermittlung von IT-Risiken

Risiko	Bereiche – Quellen - Strukturierung
Typische Risikobereiche	• Externe Umgebung • Interne Umgebung • Risikomanagement Fähigkeiten • IT Fähigkeiten • IT-bezogene Geschäftsfähigkeiten
Risiken resultieren aus	• Höherer Gewalt / Katastrophen • Technisches Versagen • Organisatorisches Versagen • Versehentliche Handlungen / menschliche Fehler • Vorsätzliche Handlungen
Eine Strukturierung der Risiken erfolgt z.B. über den Lebenszyklus eines IT-Systeme. (Die Maßnahmen können ebenfalls für diese Phasen ermittelt werden.)	• Planung, Konzeption, Architektur • Beschaffung • Umsetzung / Implementierung / Migration • Betrieb / Monitoring / Service Management • Aussonderung / Außerbetriebnahme • Notfallvorsorge / Notfallmanagement / Business Continuity

IT-Risiken – die übliche Kategorisierung

Risiko	Schäden entstehen beispielweise durch
Verlust der Vertraulichkeit	• Schadsoftware (Drive-by-Exploits (bösartige Codes, die Schwachstellen des Webbrowsers ausnutzen), Würmer/Trojaner, Exploit-Kits (anwendungsbereite Software-Pakete, die Cyberkriminalität automatisieren), u.a.m.) • Identitätsdiebstahl
Verlust der Integrität	• Manipulation von Daten (versehentlich oder vorsätzlich)
Verlust der Verfügbarkeit	• Dienstverweigerungsangriffe (DDoS-/DoS-Attacken) • Defekte der Hardware • Softwarefehler • Diebstahl und Verlust von Hardware – insb. Mobile Devices
Verlust der Nachvollziehbarkeit	• Unzureichende Beweiskraft von Transaktionen • Manipulation von – oder Fehler in Transaktionsprotokollen

Relevante internationale Normen in der ISO 2700x-Familie (Auszug)

Normen helfen bei der Ermittlung vollständiger, geeigneter und wirksamer Maßnahmen zur Behandlung der IT-Sicherheitsrisiken.

Nummer	Titel	Status
ISO 27000	Overview and vocabulary	Aktuelle Version: Dezember 2012
ISO 27001	**Information security management systems — Requirements**	**Neue Version in Vorbereitung für 2013/14**
ISO 27002	Code of practice for information security management	Neue Version in Vorbereitung für 2013/14
ISO 27003	ISMS implementation guidance	
ISO 27004	Measurement	
ISO 27005	**Information security risk management**	
ISO 27014	Governance of information security	
ISO 27013	Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	
ISO TR 27016	Information security management – Organisational economics	

ISO 27001 – die wesentlichen Kapitel

- ✓ Establishing the ISMS (4.2.1)
  - Define the scope and Boundaries of the ISMS; Define an ISMS policy; Define the risk assessment approach
  - Identify the risks; Analyze and evaluate the risks; Identify and evaluate options for the treatment of risks
  - Select control objectives for the treatment of risks
  - Prepare a Statement of Applicability
- ✓ Implement and operate the ISMS (4.2.2)
- ✓ Monitor and Review the ISMS (4.2.3)
- ✓ Maintain and Improve the ISMS (4.2.4)
- ✓ Documentation requirements – General (4.3.1); Control of documents (4.3.2); Control of records (4.3.3)
- ✓ Management commitment (5.1)
- ✓ Resource management (5.2)
- ✓ Internal ISMS audits (6.)
- ✓ Management review of the ISMS (7.)
- ✓ ISMS improvement (8.)

➢ **ISO 27001 gibt einen grobe Handlungsanleitung zur Einführung eines ISMS vor.**

Arbeitspakete zur Etablierung eines ISMS

1. Planung, Definitionen, Abgrenzungen, GAP-Analysen, Security Policy, Risikobehandlung, Maßnahmenplanung (**Phase: PLAN**)

2. Umsetzung, Prozesse etablieren (Kommunikation, Dokumentation, Verantwortlichkeiten), Maßnahmenumsetzung (**Phase: DO**)

3. interne IT-Sicherheitsrevision durchführen, Status feststellen, Erfolgskontrolle (**Phase: CHECK**)

4. Optimierung des ISMS, Umsetzung von Korrekturmaßnahmen (**Phase: ACT**)

5. Ausdehnung des ISMS auf weitere Bereiche der IT, Übergang in Betriebsprozesse, Ende des Einführungsprojekts (**Phase: EXPAND**)

Das ISMS muss nicht sofort mit der gesamten IT beginnen. Zu Beginn sollten die Aktivitäten auf die Schwerpunkte konzentriert werden. Ein neues ISMS-Team muss die Arbeit mit den vielen parallelen IT-Sicherheitsprojekten in den unterschiedlichsten Ausprägungen und Reifegraden trainieren.

➢ **Auch bei ISMS gilt: Think big - start small!**

Reifegrade des ISMS

- ✓ **Es sind ad-hoc Ansätze für Prozesse und Verfahren im Einsatz.** Prozesse und Policies sind nicht definiert.
- ✓ **Ähnliche allgemeine Prozesse entwickeln sich, basieren aber auf Intuition und individueller Expertise.**
- ✓ **Verwendung von Good Practices entwickeln sich.** Prozesse, Policies und Verfahren sind für wesentliche Aktivitäten definiert und dokumentiert.
- ✓ **Die Prozesse sind rund und vollständig.** Interne Best Practices werden angewendet. Sämtliche Aspekte der Prozesse sind dokumentiert und wiederholbar. Policies wurden vom Management freigegeben. Standards zur Weiterentwicklung der Prozesse existieren und werden befolgt.
- ✓ **Externe Best Practices und Standards werden angewendet.** Die Prozessdokumentation wurde zu automatisierten Workflows entwickelt. Prozesse, Policies und Verfahren sind festgelegt und integriert und ermöglichen ein vollständiges, durchgängiges Management und Verbesserungen.

✓ (Auszug aus dem CoBIT 4.0 Framework – Attribute der Reife für Policies, Standards und Verfahren)

➢ **Je nach Sensibilität des Unternehmens oder -bereichs, sollte ein bestimmter Reifegrad erreicht sein.**

Bewertung von IT-Risiken

Es sind verschiedene Methoden anwendbar:

- ✓ ISO 27005
- ✓ BSI Standards 100-2 und 100-3
- ✓ NIST SP800-30 R1
- ✓ Und weitere …..

Beispiel einer Matrix zur Risikobewertung:

		Wirkung				
		unbedeutend	gering	mittel	groß	katastrophal
Eintritts-wahr-schein-lichkeit	Fast sicher	mittel	bedeutend	hoch	hoch	hoch
	Wahrscheinlich	mittel	bedeutend	bedeutend	hoch	hoch
	Möglich	gering	mittel	bedeutend	hoch	hoch
	Selten	gering	mittel	mittel	bedeutend	hoch
	Sehr selten	gering	gering	mittel	bedeutend	bedeutend

➢ **Die konkreten Maßnahmen zu Erhöhung der Sicherheit müssen sich an der Wirkung einzelner Risiken orientieren.**

Eine pragmatische Risikobewertung:

- ✓ **Identifikation der bedrohten Objekte** und Abgrenzung des Analysebereichs
- ✓ **Risikoidentifikation**: Wertanalyse, Bedrohungsanalyse, Schwachstellenanalyse, Berücksichtigung bestehender Sicherheitsmaßnahmen
- ✓ **Risikobewertung**: Auswirkung und Häufigkeit gemäß eines geeigneten Bewertungsschemas
- ✓ **Risikobehandlung**: Ermittlung geeigneter und wirksamer IT-Sicherheitsmaßnahmen technischer und organisatorischer Art
- ✓ **Restrisikobewertung**: verbleibende Risiken nach Maßnahmenumsetzung zur Behandlung von Schadenhöhe und Häufigkeit
- ✓ **Priorisierung der IT-Sicherheitsmaßnahmen** als Input für die Umsetzungsplanung
- ✓ Ermittlung von Maßnahmen zum **Risikomonitoring** als Input für das Risikomanagement

Weiterführende Literatur z.B.: ISO/IEC 31000, ISO/IEC 31010, ISO/IEC 27005, NIST SP 800-30, TOGAF 9.1

➢ **Durch Anwendung der IT-Grundschutz-Vorgehensweise des BSI kann der Prozess zur Erstellung eines Sicherheitskonzepts für normalen Schutzbedarf erheblich verkürzt werden.**

Mögliche Unterstützungsleistung von SCOPAR

- ✓ **IT-Sicherheitsmanagement**
  Unterstützung bei Einführung und Betrieb eines wirksamen IT-Sicherheitsmanagements einschließlich aller dazu gehörenden Prozesse wie IT-Sicherheitsrevison mit internen Audits, IT-Risikomanagement und Dokumentenmanagement. Review, Anpassung und Aktualisierung vorhandener Dokumentationen

- ✓ **Interne Audits**
  Interne Audits, die nicht zu einer Zertifizierung führen, können durchgeführt werden. Interne Audits (GAP-Analysen, Basis-Sicherheitschecks) sind wesentliche Tätigkeiten der internen IT-Sicherheitsrevison, die innerhalb des IT-Sicherheitsmanagements durchgeführt werden.

- ✓ **Kurz-Audits und Einschätzungen**
  Gezielte Audits einzelner IT-Systeme und Prozesse in geringem Zeitrahmen aber mit vollständiger Tiefe oder auch Querschnitts-Audits bei denen die wirksame Behandlung der wichtigsten Risiken betrachtet wird. Das Ergebnis ist in jedem Fall eine priorisierte Maßnahmenliste auf Basis der individuellen Gegebenheiten.

- ✓ **Risikomanagement**
  Unterstützung beim Aufbau eines wirksamen Risikomanagement-Prozesses innerhalb des IT-Sicherheitsmanagements. Erstellung von Risikoanalysen und Risikobewertungen. Maßnahmenvorschläge zur Risikobehandlung. Je nach Sachlage können Verfahren wie ISO 27005, FMEA, FMECA, FTA oder BSI Standard 100-3 eingesetzt werden.

➢ **Die Experten von SCOPAR haben umfassende Erfahrungen in den unterschiedlichsten Fragestellungen aus dem Bereich IT-Sicherheit.**

Referenzen (Auszug)

- ✓ Audit-Vorbereitung für ein Audit zum IT-Grundschutz-Zertifikat und zur Zertifizierung gemäß ISO 27001 auf Basis IT-Grundschutz bei einer Lebens- und Sachversicherung

- ✓ Entwicklung einer IT-Sicherheitsleitlinie für eine Großforschungseinrichtung

- ✓ Audit-Vorbereitung für ein Audit analog zu einem Audit zur Zertifizierung gemäß ISO 27001 auf Basis IT-Grundschutz für eine Behörde:

    - Vollständige Anwendung der IT-Grundschutz-Vorgehensweise

    - Strukturanalyse, Schutzbedarfsfeststellung, Modellierung, Basis-Sicherheitscheck, Ergänzende Sicherheitsanalyse, ergänzende Risikoanalyse

    - Erstellung von Richtlinien als Bindeglied zwischen der Sicherheitsleitlinie und den Feinkonzepten und als Arbeitsgrundlage für IT-Sicherheitsmanagement und IT-Revision

Gerne helfen wir auch Ihnen, erfolgreicher zu sein ..

Beratung

Coaching *Lösungen*

Strategie *Konzeption*

SCOPAR

Reviews *Gutachten*

Trainings *Seminare*

Umsetzung

SCOPAR GmbH
Klara-Löwe-Straße 3 * D - 97082 Würzburg
Fon: +49 - 931 - 45320500 * Fax: +49 - 931 - 45320505
E-Mail: knauf@scopar.de * Web: www.SCOPAR.de