Hacking Day 2013 – Security Lifecycle

Griffige Information Security Policies
Balance zwischen Theorie und Praxis

Yves Kraft – Team Leader Consulting & Training – OneConsult GmbH

Beamte konsumierten Porno am Arbeitsplatz

DELSBERG – Rund 30 Angestellte des Kantons Jura sollen während der Arbeit Sexseiten im Internet besucht haben. Die Regierung hat eine Untersuchung eingeleitet.

14. Januar 2013 - Blick

Hacker-Attacke auf SRF

ZÜRICH - Das Schweizer Radio und Fernsehen ist Ziel einer Cyberattacke geworden. Daher sind seit gut einer Woche SRF-Blogs und Foren nicht verfügbar.

08. März 2013- NZZ

Datenklau bei Julius Bär: Anklage noch im Mai

ZÜRICH - In den Fall des Datendiebstahls bei Julius Bär kommt Bewegung: Gegen den verhafteten deutschen IT-Spezialisten soll spätestens Ende Mai Anklage erhoben werden.

25. März 2013 - Handelszeitung

Agenda

- → Vorstellung
- → Theorie
- → Balance in der Praxis
- → Zertifizierung

Über mich

- → Yves Kraft
- → Team Leader Consulting & Training
- → Theorie
  - Informatiker
  - Studium BSc FH CS (Vertiefung IT-Security)
  - OPST, OPSA, OSSTMM Trainer
- → Praxis
  - 11 Jahre Berufserfahrung , davon 4 Jahre in IT-Security
  - System Engineer & System Administrator
  - Technische Security Audits
  - Konzeptionelles Consulting
  - Security Officer
  - Training & Coaching

Dienstleistungen

→ Security Audits 60%

- Security Scan
- Penetration Test
- Application Security Audit
- Ethical Hacking
- Social Engineering
- Conceptual Security Audit

→ Consulting 20%

- Strategy & Organisation
- Policies & Guidelines
- Processes & Documentation
- Business Continuity & Disaster Recovery
- Engineering & Project Management

→ Incident Response 10%

- Emergency Response
- Computer Forensics

→ Training & Coaching 10%

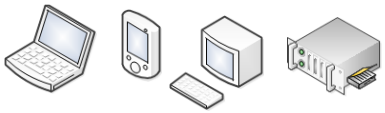
- OSSTMM Zertifizierungskurse
- Practical Security Scanning
- Secure Web Development
- Coaching

→ Security as a Service

Agenda

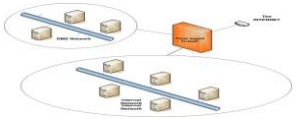
- → Vorstellung
- → Theorie
- → Balance in der Praxis
- → Zertifizierung

Übersicht Information Security

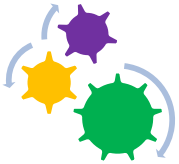


Infrastruktur

Dokumente



Netzwerk Segmente

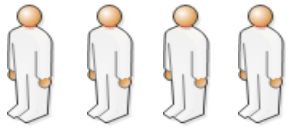


Prozesse

Information Security

Organisation

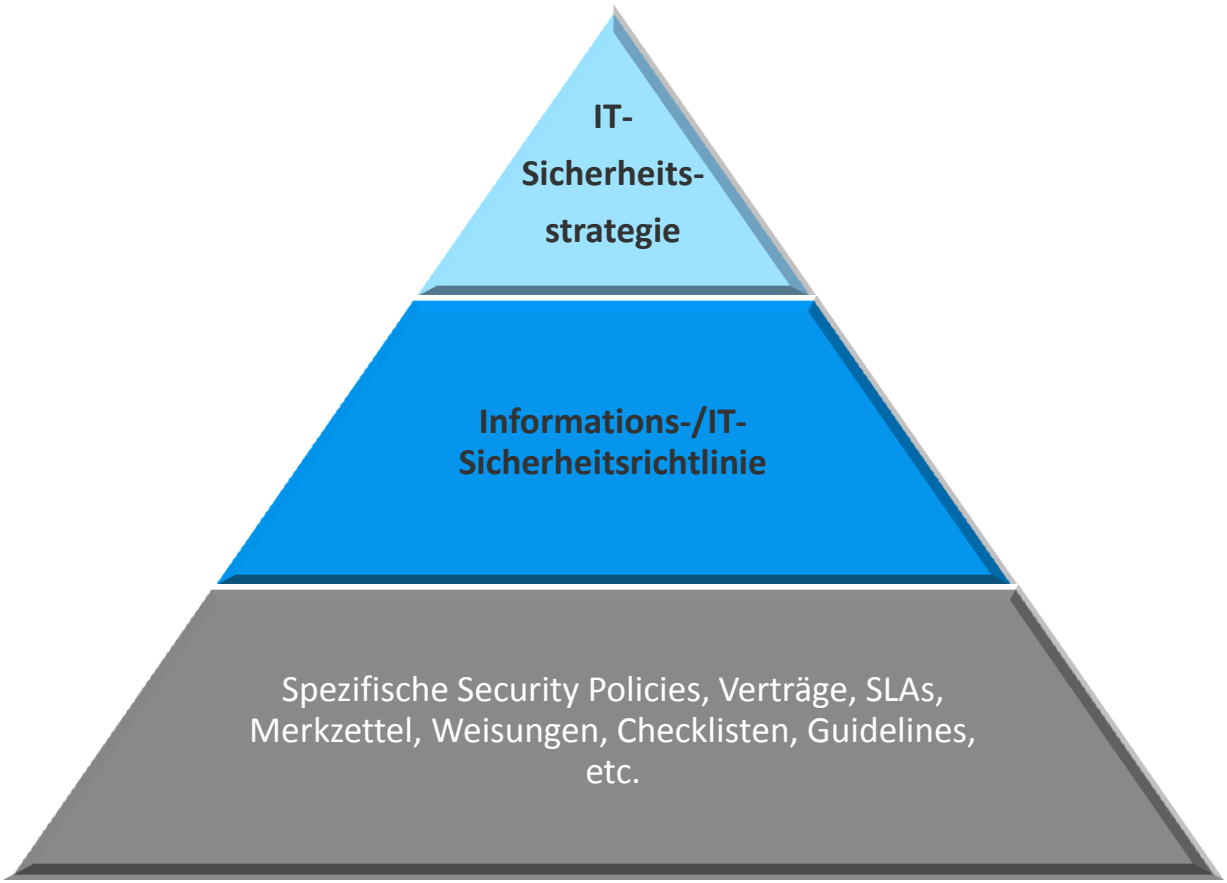
Daten



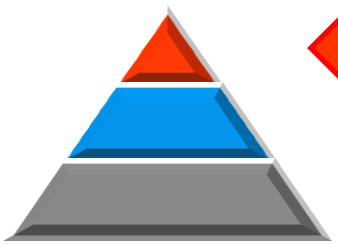
Human Resources

Compliance

Übersicht Information Security

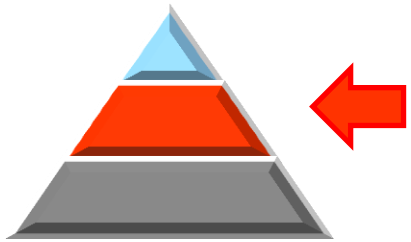


IT-Sicherheitsstrategie



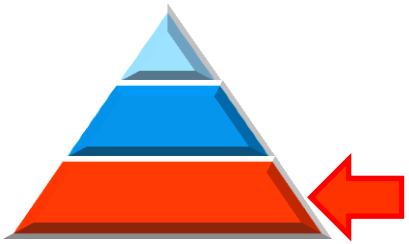
- Generelles Dokument zur Planung, Gewährleistung und ständigen Aufrechterhaltung der IT-Sicherheit
- Festlegungen werden zumeist zu IT-Sicherheits-Policies/IT-Sicherheitsleitlinien
- IT-Sicherheitsstrategien beinhalten u.a.
  - Angaben den lokalen Zielen der IT-Sicherheit
  - Zugrunde liegenden Sicherheitsstandards (z.B. IT-Grundschutz, ISO 27001)
  - Festlegung von Sicherheitsdomänen
  - organisatorischer Aufbau des Sicherheitsmanagements
  - Berichtspflichten und Kontrollinstanzen
  - Qualitätssicherung

IT-Sicherheitsrichtlinie



- → Verfolgt die IT-Sicherheitsstrategie
- → Ziele und Massnahmen zur Umsetzung der Informationssicherheit
  - Stellenwert der Informationssicherheit
  - Benennung der Sicherheitsziele
  - Beschreibung der Organisationsstruktur
  - Auf Leitungsebene durchsetzen und Verstösse sanktionieren
  - Periodische Überprüfung der Sicherheitsmassnahmen
  - Erhalt und Förderung der Security Awareness durch Schulungs- und Sensibilisierungsmassnahmen
  - Verantwortlichkeiten im Informationssicherheitsprozess

Policies, Checkliste, Guidelines



→ Spezifische Security Policies
- Verträge & SLAs
- Merkzettel
- Weisungen
- Checklisten
- Guidelines

→ Beispiele: Betriebshandbücher, Installationsanleitungen, Hardening Guides, Gebäudepläne

Normen und Standards

- → ISO/IEC 27000 Reihe
  - ISO 27000 – Begriffe und Definitionen
  - ISO 27001 – Anforderungen für Sicherheitsmechanismen
  - ISO 27002 – Code of Practice
  - ISO 27005 – Risk Management
- → BSI Standard 100-1/4 (eh. Grundschutzhandbuch)
- → Weitere
  - COBIT
  - SOX
  - PCI-DSS
  - …

Agenda

- → Vorstellung
- → Theorie
- → Balance in der Praxis
- → Zertifizierung

Was will ich erreichen?

→ Informationssicherheit dient dem Schutz
- Gefahren bzw. Bedrohungen
- Vermeidung von Schäden
- Minimierung von Risiken

→ Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen

Bedrohungen in der Praxis

- → Irrtum und Nachlässigkeit
- → Malware
- → Social Engineering
- → Hacking
- → Wirtschaftsspionage
- → Diebstahl von IT-Mitteln

Probleme in der Praxis…

- → Resignation, Fatalismus und Verdrängung
- → Kommunikationsprobleme
- → Sicherheit wird als rein technisches Problem mit technischen Lösungen gesehen
- → Zielkonflikte: Sicherheit, Bequemlichkeit, Kosten
- → Ad-hoc Vorgehen (unter Zugzwang) bzw. falsche Methodik
- → Management: fehlendes Interesse, schlechtes Vorbild
- → Sicherheitskonzepte richten sich an Experten

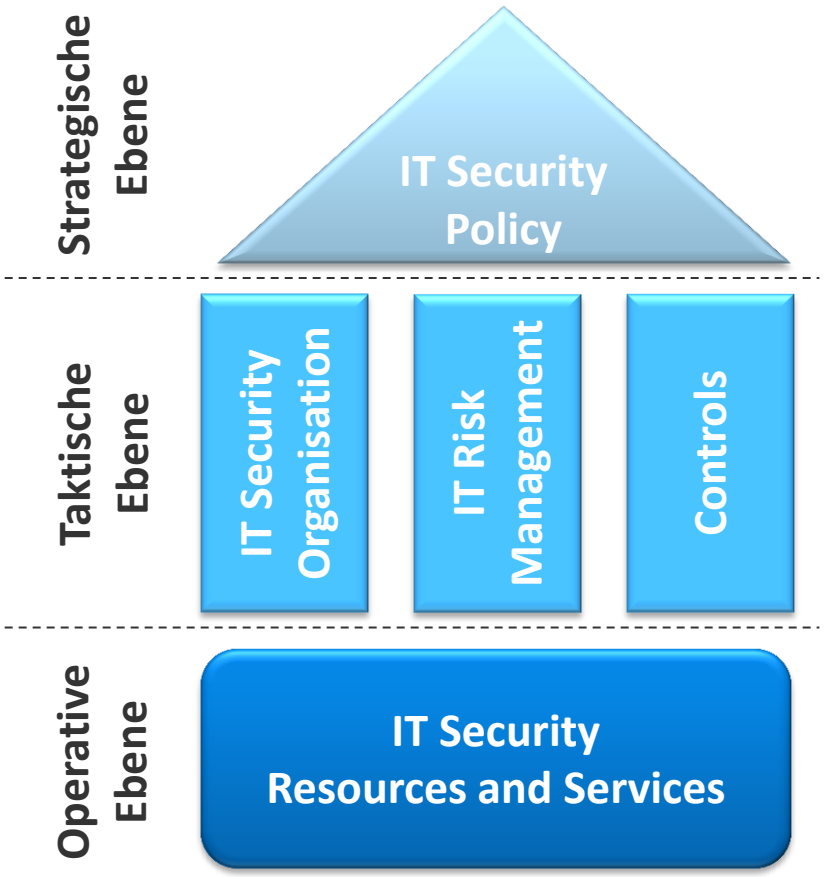
Probleme im Zusammenhang mit Policies…

- → Policies sind nicht individualisiert
- → Policies sind nicht umsetzbar
- → Freigabe, Bekanntmachung und Zielgruppe werden vergessen
- → Policies werden nicht aktualisiert

…und die Konsequenzen

- → Konfusion im Notfall
- → lückenhafte Datensicherung
- → fehlende Klassifizierung von Informationen
- → gefährliche Internetnutzung
- → Disziplinlosigkeit

Implementation nach ISO 2700x



- → IT Security Policy
  Anforderungen an ISMS
- → IT Security Organisation
  Organisationsstrukturen, Prozesse, Regelungen
- → IT Risk Management
  Ermittlung von Risiken von Komponenten und deren Auswirkung
- → Controls
  Sicherheitsmechanismen
- → IT Security Res. & Services
  Technologien, Anlagen, Anwendungen, Personal

Grundvoraussetzungen

→ **Awareness:** Geschäftsleitung anerkennt IT-Security als notwendiger Faktor

→ **Commitment:** Geschäftsleitung

- spricht die finanziellen und zeitlichen Ressourcen
- unterstützt das Projekt

Inhalt & Sprache von Richtlinien

- → Zielgruppenorientierung
  - Zielgruppe(n) Geschäftsleitung, IT-Abteilung, Mitarbeiter und/oder weitere Stakeholder/Interessenten
  - Akademischer Schreibstil vs. möglichst nahe an der Umgangssprache
  - Sprache: Deutsch oder Englisch
- → Aufbau/Dokumentenstruktur
  - rein direktive Vorgaben vs. detaillierte Erläuterungen der Entscheide
  - umfassendes Dokument vs. Hauptdokument mit Anhängen oder Beilagen
- → Umfang und Etappierung
  - Kurzversion: ca. 2 - 5 Seiten
  - Langversion: ca. 15 - 40 Seiten
  - Erstellung aller Dokumente in einem Zug vs. etappierte Erstellung (z.B. Kurzversion und danach Voll-/Langversion)

Agenda

- → Vorstellung
- → Theorie
- → Balance in der Praxis
- → Zertifizierung

Anerkannte Standards

- BS 25999-2:2007
- BSI Standard 100-1/4 (eh. Grundschutzhandbuch)
- ISO/IEC 27001:2005
  Zertifizierung von Informationssicherheits-Managementsystemen (ISMS)

Motivation für eine Zertifizierung

- → Differenzierung im Wettbewerb
  - Managementkompetenz im Bereich Informationssicherheit
  - Zuverlässigkeit als Partner
  - Sich von der Konkurrenz abheben (Zertifikat ist kein Massenprodukt)
- → Interner Nutzen einer Zertifizierung
  - Mögliche Verluste Infolge von Sicherheitsschwachstellen minimieren
- → Vorschriften
  - Derzeit keine gesetzlichen Anforderungen betreffend zwingender Zertifizierung
  - aber: Sorgfaltspflicht, Datenschutzgesetz, etc.

Der Weg zur Zertifizierung (ISO/IEC 27001)

- → Stufe 1: Dokumentenprüfung (teils vor Ort)
- → Stufe 2: Audit vor Ort
- → Auditbericht und Zertifikat mit 3-jähriger Gültigkeit
- → Überwachungsaudits nach dem ersten und zweiten Jahr
- → Re-Zertifizierung nach dem dritten Jahr
- → Überwachungsaudits nach dem vierten und fünften Jahr
- → …

Tipps betreffend Zertifizierung

- → Normverständnis schaffen
- → Verfügbarkeit aller notwendigen Dokumente sicherstellen
- → Enge Zusammenarbeit mit der Zertifizierungsstelle
- → «Klassische» Prüfpunkte beachten und so Fehlerquellen beseitigen
- → Nachbesserungsfrist sinnvoll nutzen und Termine einhalten
- → Nach dem Audit ist vor dem Audit

Beamte konsumierten Porno am Arbeitsplatz

DELSBERG – Rund 30 Angestellte des Kantons Jura sollen während der Arbeit Sexseiten im Internet besucht haben. Die Regierung hat eine Untersuchung eingeleitet.

14. Januar 2013 - Blick

Hacker-Attacke auf SRF

ZÜRICH: Das Schweizer Radio und Fernsehen ist Ziel einer Cyberattacke geworden. Daher sind seit gut einer Woche SRF-Blogs und Foren nicht verfügbar.

08. März 2013- NZZ

Datenklau bei Julius Bär: Anklage noch im März

ZÜRICH: Im Fall des Datendiebstahls bei Julius Bär kommt Bewegung: Gegen den verhafteten deutschen IT-Spezialisten soll spätestens Ende März Anklage erhoben werden.

25. März 2013 - Handelszeitung

NUTZUNGSRICHTLINIE

DISASTER RECOVERY

BUSINESS CONTINUITY

NUTZUNGSRICHTLINIE

ZUGANGSKONTROLLE

«Sicherheit ist kein Produkt, sondern ein Prozess»

Bruce Schneier

Danke für Ihre Aufmerksamkeit! Fragen?

Yves Kraft
BSc FH CS, OPST&OPSA
Team Leader Consulting & Training

yves.kraft@oneconsult.com
+41 79 308 15 15

Hauptsitz
OneConsult GmbH
Schützenstrasse 1
8800 Thalwil
Schweiz

Tel +41 43 377 22 22
Fax +41 43 377 22 77
info@oneconsult.com

Büro Deutschland
Niederlassung der OneConsult GmbH
Karlstraße 35
80333 München
Deutschland

Tel +49 89 452 35 25 25
Fax +49 89 452 35 21 10
info@oneconsult.de

Büro Österreich
Niederlassung der OneConsult GmbH
Wienerbergstraße 11/12A
1100 Wien
Österreich

Tel +43 1 99460 64 69
Fax +43 1 99460 50 00
info@oneconsult.at