T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 02. - 03.11.2015

Einsparungen und Informationssicherheit – ein Widerspruch?

Axel Leitner

Aritron

Vorstellung

Selbständiger IT Berater seit über 12 Jahren:

Schwerpunkte:

- Systeme, Netzwerke
- Cyber-Security
- ISMS und Compliance

- Consultant & Projektleiter

Ausgangslage

Kosten von Informationssicherheitsprojekten und Betrieb

- Hoher Invest und Entwicklungsauswand
- Höher Aufwand für Überzeugungs- und Beratungsarbeit
- Hohe organisatorische Komplexität des Projektes
- Schwierige Budgetplanung
- schwierige Planung und Verfügbarkeit von Ressourcen
- Viele Kopfmonopole
- Spezielle Anforderungen an eingesetzte Hilfsmittel
- Umfangreiche Prozeßgestaltungen als Folge eines ISMS
- Hohe Aufwände an die Vorbereitung und Übergabe an Betriebs-Einheiten
- Aufwändige Auditplanung und Erhaltung im Betrieb

Projekt

Aus der Sicht von IS Projekten

Was ist zu schützen – Werte!

Beginn mit Schutzbedarfsfeststellung bzw. Datenklassifizierung.

Wichtige Phasen
- Vorbereitung: Planung Budget und Ressourcen
- Umsetzen
- Kontrolle
- Übergabe

Einige Erfahrungen

SiBe Orga hat weiterhin Nachholbedarf
(KES Studie 2012: nur ca. ¾ großer Unternehmen hat ISO)

IPSEC VPN vs Web/SSL Remote Zugriffe

Lieferketten und Outsourcing – das schwächste Glied

Im Focus: Mobile Security

Einige Bedrohungen

- Im Jahr 2000 gab es www Argumente in der Beratung, jetzt sind die Gefährdungen und Schäden bei jedem präsent. (Massendatenverluste, Schäden in Industrieprodukten, nicht deckende Versicherungen)
- Hauptbedrohungen: Drive-by, DDOS, gezielt (USB, email)
  - Zu über 50% unbeabstichtigtes Fehlverhalten von Mitarbeitern für erfolgreiche Angriffe verantwortlich (quo vadis awareness)
  - Zahlreiche „grosse“ Angriffe über Fernzugriffe
  - Jedoch unter 20% Innentäter (vorsätzlich), trotzdem fürchten sich immer noch über 30% vor Innentätern

  (Quelle: BSI Cyber-Sicherheits-Umfrage 2015)

Maßnahmen

- Hauptbedrohungen: Drive-by, DDOS, gezielt (USB, email)
- Maßnahmen Umsetzung prüfen mit Schwachstellenscans
- IT Risiken Lage-/Umsetzungsplan erstellen und Überwachung verstärken in schwachen Bereichen, Beispiel
- Elementare Konfigurationen überwachen mit SIEM (mindestens normale Servicezeiten)
- Beispiel maliziöser Verkehr: Investition in neuere kognitive Firewallsysteme
- Maßnahmen haben Einfluss auf andere Projekte, Empfehlung: Projekt Security Berater vom Anfang ausreichend einplanen!

Besonderheiten bei IT Security Projekten

- Personalerfordernisse
  - Strafregisterauszug, Geheimschutz
- Vertrauen in HW & SW Auswahl unterschiedlicher Einflußzonen
- Nachverfolgung von Änderungen bei
  - regulatorischen Anforderungen
    Beispiele
  - Änderungen in der Bedrohungslage
  - Änderungen von Geschäftsrisiken
- Code Review
- Aufgabenverteilung ins Ausland
- Erhöhte Beratungsleistung für Manager

Einflussfaktoren Mitarbeiter

- Projektleiter, bevorzugt langjähriger Mitarbeiter des Unternehmens, der die Organisation und Fachbereiche kennt
- IS Projekte meistens höhere 2-stellige Prozentanteil von externen Beratern
- Beratungsunternehmen vs Freiberufler
  - Einfluss von Betriebsrat, Scheinselbständigkeit, Kosten
- Verfügbarkeit von Ressourcen bzw. Ingenieuren und Beratern
- Interne Mitarbeiter: Voll- oder Teilzeit im Projekt
  - Problem der Verfügbarkeit (Überstunden, Betriebsrat)
  - Vorteil der Kenntnis der Geschäfts- und Betriebsprozesse
- „Kunst“ Berater zu halten nicht nur bei Freiberuflern
- Überwiegend „kritische Ressource“, oft nicht ersetzbar

Einflussfaktoren IT Governance, Risk und Compliance

- Begrifflichkeiten: ISMS, CSMS, GRC
- CISO, der Compliance im „Griff“ hat.
    - 90% der CISOs sind von Maßnahmen überzeugt
    - Nur 10% der IE Anwender nutzen aktuelle Versionen
    - <50% funktionsfähiges Patchmanagement

    (lt. Cisco Annual Security Report 2015)
    - bei 99,9% der ausgenutzten Schwachstellen wurde der CVE bereits mind. ein Jahr davor veröffentlicht (Verizon, DBIR 2015)
    - 76% of vulnerabilities are over two years old. (NTT, GTIR 2015).
- Einfluss interner und externer Revision (Verständnis Compliance)
- Manager Entscheidungen schwierig abzustimmen
- Outsourcing: Schnittstellen ISMS, Interpretationen regul. Anf.

Budget und Prozesse

- Projektaufwände Beratung/Entwicklung
- Investitionen HW/SW
- Investitionszyklen
- Lizenzen
- Audit
- Viele Querschnittsthemen in der IS
- Schwierige Budget und Ressourcenplanung (Verfügbarkeiten)
- Projektbudget +20% für Security Maßnahmen
- Fachabteilung vorzeitig aufstocken für Projektunterstützung
- Betriebsanforderungen: beispielsweise SOC bei IPS/SIEM
- Hohe Anforderungen an Betriebsprozesse
    - Beispiel: 802.1x, IMAC/R

Projektrisiken

- Festlegen des Verbundes (besonders anfällig für scope creep)
- Explodierende Projektkosten
- Nicht durchgeführte Schutzbedarfsanalyse bzw. BIA & Risikoanalyse, Vorteil: Grundschutz Gefährdungen
- Akzeptanz, Hierachien und Weisungsbefugnis
- Verschlüsselung: z.B. Änderungen der Algorithmuskriterien Zusätzlicher Entwicklungsaufwand
- Ungeplante Betriebskosten bis zur nicht Betreibbarkeit
  Extrembeispiele:
  - pseudo Inbetriebnahme mit Testsystemen
  - Hohe false negatives bei IPS, Firewall auch nach Jahren mit „any any allow“

Betrieb

- Aufrechterhaltung des ISMS
- Revision und Aktualisierung der Richtlinien
- Aktualisierung der Fachkonzepte und SIKOs
- Mehraufwand in Fachabteilungen bei neuen Sicherheitssystemen
- Betriebsübergabe Erfordernisse teilweise sehr aufwändig zu erfüllen
- Kontrollanforderungen (z.B. Eventanalyse) SOC kostspielig

Spezielle Aufwände nach Zertifizierung:

- Vorbereitungen des Überwachungsaudits
- Dokumentation der Änderungen und Abstimmung mit der Zertifizierungsstelle
- Aufwände durch Änderungen im zugrundelegenden Standard

GRC Programm

Vorteile eines Tools:

- Aktuelle Standards
- Methodische Hilfe (verschiedene Standards)
- gleichzeitige Bearbeitung und Benutzerverwaltung
- Revisionssicherer Betrieb (verschlüsselte Verbindung und Daten)
- zentrale Kontrolle des Prozesses – Einsparungen bei Aufrechterhaltung
- Auditkosten Einsparung, da vorgefertigte ISMS Standard Berichtsformate
- Synergien bei Verwendung des Tools für mehrere Standards

Nachteile Tools:

Implementierungskosten, Herstellerbindung

Fazit

- Werte kennen und Maßnahmen nach Schutzbedarf umsetzen
- ISO – Umhängen und Aufstocken
- Funktionierendes Patchmanagement
- Einsatz eines GRC Programms
- Fernzugriffe nach Schutzbedarf
- Lieferketten und Outsourcing – Vertragliche Regelung hilft wenig, ISMS Zertifizierung auch nicht immer, Risiko aufzeigen

Fragen und Diskussion

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Axel Leitner
Unternehmensberater IT
Schleißheimer Straße 398
80809 München
axel.leitner(a)aritron.de
Telefon: +49 89 189 11 959