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

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Berlin, 06. - 07.11.2018

IT-Sicherheitszertifizierung: Projekterfahrungen

Thomas Wallutis, @-yet GmbH

Über mich

- Diplom-Mathematiker
- IT Security seit 2003
- T.I.S.P. seit 2009
- Herstellerunabhängige IT Security Beratung
- Serverüberwachung (Nagios/Check_MK)
- IT-Infrastrukturdokumentation (i-doit)
- …und noch mehr

Agenda

- Motivation
- Vor dem Start
- Der Start
- Richtlinien
- Dokumentation
- Maßnahmen und Controls
- Vor-Ort-Audit
- Nach dem Audit
- Fazit

Motivation

- 2015/2016: Projekt zur Zertifizierung nach ISO27001
- 2016/2018: Projekt zur Zertifizierung „ISO27001 auf Basis von BSI Grundschutz“ („alte“ Version“)
- 2016/2017: Beschäftigung mit VdS 10000 (ehemals VdS 3473)
  - Anmerkungen beziehen sich noch auf VdS 3473

Motivation

- Beratung bei Fragen
- Erstellung von Richtlinien
- Bearbeitung von Maßnahmen (BSI GS)
- Begleitung beim Vor-Ort-Audit

Vor dem Start

- Warum soll das Projekt durchgeführt werden?
- Es handelt sich um einen Prozess, nicht um ein Projekt
  - In der Zukunft wird das ISMS Zeit beanspruchen (Dokumentenpflege, Notfallübungen etc.)
- Nicht nur das Kernteam wird beansprucht
- Frühzeitig mit Maßnahmen bzw. Controls beschäftigen

Vor dem Start

- Tools
  - Excel
  - i-doit

- Nutzen Sie etwas, dass Ihnen nicht noch zusätzliche Mühe macht

Vor dem Start

- Es wird ein Management System zertifiziert
- Die IT-Sicherheit wird implizit mit überprüft (insbesondere beim „alten“ BSI Grundschutz)
- Es geht um gewollte (Hacker) und ungewollte (Hardwareausfall) Störungen der Informationssicherheit
- Im Mittelpunkt stehen Informationen, nicht Systeme

Vor dem Start

- Haben Sie den Fehler auf der vorherigen Folie bemerkt?

- Informationssicherheit, nicht IT-Sicherheit!

Der Start

Das Team zusammenstellen

Der Start

- Das Team
  - Kernteam
  - Erweitertes Kernteam
  - Ansprechpartner in den betroffenen Abteilungen

- Kernteam
  - Interner Mitarbeiter (Projektverantwortlicher)
  - Externe Mitarbeiter (Projektverantwortlicher + Unterstützung)

Der Start

- Erweitertes Kernteam
  - Auditor (zur Beratung)
  - IT-Leiter
  - Geschäftsleitung

- Ansprechpartner
  - Bereitstellung von Dokumenten
  - Ansprechpartner bei Fragen
  - Schnittstelle zu Externen (Dienstleister, Hoster etc.)

Der Start

- Leitlinie erstellen
- Zeitplan erstellen
  - Ansprechpartner müssen wissen, welcher Aufwand zu welchem Zeitpunkt auf sie zukommt
  - Abgleich mit anderen Projekten
- Kosten- und Aufwandskontrolle implementieren

Der Start

- Informieren Sie alle Beteiligten frühzeitig, welche Informationen zusammengestellt werden müssen

- Dokumentation
  - Nicht zwingend in gewünschter Form vorhanden
  - Aktuell?

Der Start

- Scope betrachten
  - Je nach Zertifizierung werden sehr detaillierte Fragen gestellt
  - Können die Fragen in gewünschter Tiefe beantwortet werden?

- Wichtige Geschäftsprozesse identifizieren

Der Start

- Business Impact Analyse
  - Wurde im Projekt erst durch den Auditor angefordert
  - Besser: direkt machen!

- Schutzbedarf festlegen
  - Höherer Schutzbedarf bedingt u.U. erweiterte Maßnahmen
  - Mit Geschäftsleitung abgleichen

Der Start

- Risikoanalyse
  - Risiken bewerten
  - Behandlungsoptionen auswählen
  - Risikobehandlungsplan aufstellen

- Vorgehensweisen
  - BSI 200-3
  - ISO/IEC27005

- Siehe auch: https://advisera.com/27001academy/de/knowledgebase/iso-27001-risikobewertung-und-risikobehandlung-6-grundlegende-schritte/

Richtlinien

Richtlinien

- Welche Richtlinien werden gefordert?
- Richtlinien sind Einzelanweisungen immer vorzuziehen
- Aktualität

Richtlinien

- Wer schreibt was?

- Richtlinien ziehen Aktionen nach sich
  - Clean Desk Policy
  - Kryptographie

- Richtlinien von Geschäftsführung abzeichnen lassen
  - Erspart unnötige Diskussionen

Richtlinien

- Kernrichtlinien
  - Dokumentenklassifizierung
  - IT-Sicherheitsrichtlinie
  - Administrationsrichtlinie
  - Richtlinie zur Notfallvorsorge/-behandlung
  - Incident Response Richtlinie

- Zielgruppenspezifisch schreiben

Richtlinien

- Was soll durch die Richtlinien geregelt werden?
  - Die BSI Grundschutzkataloge sind sehr detailliert und eine gute Quelle
  - Vds10000 und ISO27002
  - Herstellerempfehlungen (als Umsetzungshilfe)

- Nicht zu viel am Anfang
  - Steht es in einer Richtlinie, müssen Sie es auch umsetzen

Richtlinien

- Beachten Sie die Auswirkungen
  - Unterschied zwischen „Soll“ und „Muss“
  - Leiten sich daraus Änderungen an der Infrastruktur oder den Arbeitsweisen ab?

- Betriebs- oder Personalrat einbinden
  - Ändern sich Arbeitsabläufe?
  - Protokollierungsrichtlinien

Richtlinien

- Abgrenzung Richtlinie <-> Konfigurationsanweisung
  - Ziel vs Weg

Richtlinien

- Nach Genehmigung veröffentlichen (z.B. Intranet)
- Rechnen sie mit Kommentaren wie:
  - Aber das dauert alles sooooooooooo lange
- Auf den Hinweis:

  „Bitte nehmen Sie sich die Zeit, die Dokumente zu sichten“

Richtlinien

Richtlinien

- Nutzen Sie Vorlagen aus dem Netz
  - Formulare für Incident Response (BSI, SANS, NIST)
  - Veröffentlichte Richtlinien

- Tipp: https://advisera.com/27001academy/de/

- Dokumentvorlagen

Richtlinien

- Anforderungen an eine Richtlinie(aus VdS 10000)
  - Eine Richtlinie enthält, für wen sie verbindlich ist
  - Sie begründet, warum sie erstellt wurde und legt fest, was mit ihr erreicht werden soll
  - Sie verstößt nicht gegen die IS-Leitlinie oder andere Richtlinien
  - Sie weist auf die Konsequenzen ihrer Nichtbeachtung hin

Richtlinien

- Sagen Sie nie vorschnell „diese Richtlinie benötigen wir nicht“
  - Richtlinie für mobiles Arbeiten
  - Entwicklerrichtlinie

Dokumentation

Quelle: Wikipedia **"Photo by DAVID ILIFF. License: CC-BY-SA 3.0"**

Dokumentation

- Systemdokumentationen
  - Rahmen vorgeben
  - Rechnen Sie mit mehreren Anläufen
  - Die Detailtiefe muss sich mit den umzusetzenden Maßnahmen decken

- Notfallvorsorge
  - Wiederanlauf- und Wiederherstellungspläne
  - Wer macht was und wie lange dauert das
  - Recovery Point Objective und Recovery Time Objective

Dokumentation

- Wer ist wofür verantwortlich?
  - Besonders interessant beim Hosting oder bei Tochterunternehmen

- Welche Daten werden verarbeitet?
  - Wo liegen welche Daten?
  - Über welche Kanäle werden Daten übertragen?

Dokumentation

- Was müssen Sie an wen abgeben?
  - Auditor
  - Zertifizierungsstelle
- BSI Grundschutz
  - Referenzdokumente A.0-A.7
  - Der Basischeck muss dem BSI nicht vorgelegt werden (nur dem Auditor)
- Was darf weitergegeben werden?
  - Serviceverträge

Dokumentation

- Bereinigter Netzplan
  - Daten, Schutzbedarf und Zuständigkeiten
- Formulare
  - Benutzeranlage, Veränderung, Löschung
  - Incident Response
- Beschaffung
  - Pflichtenheft
  - Lastenheft
  - Auswahloptionen
  - Begründung der Entscheidung

Dokumentation

- Interviews
  - Planen Sie mehrere Runden ein
  - Fragen Sie hartnäckig nach
  - Oft existiert Wissen nur in Köpfen (manchmal nur in einem Kopf)

- Dokumentiertes Wissen kann in einem Notfall den Unterschied zwischen Erfolg und Misserfolg ausmachen

- Wie wollen Sie sinnvollen Schutz aufbauen, wenn Sie gar nicht wissen was Sie schützen wollen?

Maßnahmen und Controls

- Beschäftigen Sie sich frühzeitig mit dem Thema

- Wie groß ist Ihr „Risikoappetit“?
  - Die Geschäftsleitung muss Entscheidungen treffen

Maßnahmen und Controls

- ISO27001: lesen Sie die ISO27002
- BSI GS alt: sehr detailliert
- BSI GS neu und VdS 10000
  - MÜSSTE, SOLLTE etc.

Maßnahmen und Controls

- Outsourcing
  - ISO27001: Lieferantenrichtlinie
  - BSI GS (alt): Outsourcing Whitepaper von 2004
  - VdS10000: knapp gehalten; Einschränkung auf „Zugriff auf kritische Informationen“ beachten

- Diskussionspunkt (BSI GS): reichen Serviceverträge/SLAs oder muss die Massnahmenumsetzung dokumentiert werden?

Maßnahmen und Controls

- Mitarbeiterschulungen
  - Regelmäßig
  - Messbares Ergebnis

- Umsetzung
  - Am Arbeitsplatz oder in einem Schulungsraum
  - Web-basiert oder Unterlagen
  - Prüffragen

Maßnahmen und Controls

- Informationssicherheitsmanagementsystem
  - Messgrößen
    - Was sind meine (messbaren) Ziele?
  - Reviews
    - Wie stelle ich Abweichungen fest und wie vergleiche ich Überprüfungen?
  - Überarbeitung/Verbesserung

- Das CA aus PDCA!

Vor Ort Audit

Vor Ort Audit

- Lesen Sie Ihre Dokumente und Richtlinien noch einmal durch

- Instruieren Sie alle Mitarbeiter
  - Clean Desk Policy
  - Serverraum-Zutritt
  - Kennen alle die Dokumentenklassifizierung?

Vor Ort Audit

- Jeder Auditor hat ein eigenes Steckenpferd
  - Es gibt Bereiche, die er überprüfen muss
  - Und es gibt sein Spezialgebiet

- So lange Sie ihre Entscheidungen gut begründen können und sie nicht zu risikobereit sind, ist alles ok

Nach dem Audit

- Nach dem Audit ist vor dem Audit

- Sprechen sie frühzeitig darüber, wie sie nach dem Audit weitermachen wollen
  - Aufrechterhaltung des Erreichten
  - Folgeprojekte (z.B. SIEM zur Protokollierung)

Nach dem Audit

- Pflegen Sie die Dokumentation
  - Erinnern Sie Verantwortliche regelmäßig an diese Aufgabe
- Füllen Sie Lücken
- Scope im Auge behalten
  - Inwieweit beeinflussen Änderungen die Zertifizierung?

Fazit

- Ein anderer Blick auf IT
  - Organisatorische Seite
  - Lifecycle

- Detaillierterer Blick
  - Besseres Verständnis
  - Hilfreich auch für das Troubleshooting

Fazit

- Zertifizierung: ja oder nein?
  - Einzelfallentscheidung

- Aber…
  - …auch wenn Sie die Zertifizierung nicht anstreben: gehen Sie den Weg auch ohne sie