Wie erkläre ich das dem Chef?

Informationssicherheits-Risiken identifizieren und berichten

Riechen Consulting GmbH www.riechen.consulting +49 351 2684949

Agenda

Anforderungen 3

Grundschutz nach 200-2 10

Risikoanalyse nach 200-3 13

Management-Report 21

Anforderungen

Anforderungen an ein ISMS

- BSI-Standard 200-1

  Das ISMS legt fest, mit welchen Instrumenten und Methoden die Leitungsebene die auf Informationssicherheit ausgerichteten Aufgaben und Aktivitäten nachvollziehbar lenkt.

- ISMS.1.A12 Management-Berichte zur Informationssicherheit (S)

  Die Institutionsleitung SOLLTE sich regelmäßig über den Stand der Informationssicherheit informieren, insbesondere über die aktuelle Gefährdungslage sowie die Wirksamkeit und Effizienz des Sicherheitsprozesses.

Anforderungen an Management-Berichte

- ISMS.1.A12 Management-Berichte zur Informationssicherheit (S)
  - Dazu SOLLTEN Management-Berichte geschrieben werden, welche die wesentlichen relevanten Informationen über den Sicherheitsprozess enthalten, insbesondere über Probleme, Erfolge und Verbesserungsmöglichkeiten.
  - Die Management-Berichte SOLLTEN klar priorisierte Maßnahmenvorschläge enthalten. Die Maßnahmenvorschläge SOLLTEN mit realistischen Abschätzungen zum erwarteten Umsetzungsaufwand versehen sein.

… und damit die Schuldfrage geklärt ist:

- Die Management-Berichte SOLLTEN revisionssicher archiviert werden.
- Die Management-Entscheidungen über erforderliche Aktionen, den Umgang mit Restrisiken und mit Veränderungen von sicherheitsrelevanten Prozessen SOLLTEN dokumentiert sein.
- Die Management-Entscheidungen SOLLTEN revisionssicher archiviert werden.

Kunde 1

- ISB seit 3 Jahren benannt
- 10 T€ Jahresbudget
- Strukturanalyse soll beauftragt werden
- Schutzbedarfsfeststellung machen wir dann nächstes Jahr
- Behördenleitung:

Kunde 2

- Regelmäßige Audits (KRITIS)
- Audit-Report = Umsetzungsplanung
- Nächstes Audit: noch mehr Abweichungen
- Vorstand:

Kunde 3

- ISB präsentiert der Geschäftsführung Bericht A.4 mit 6000 Seiten
- GF: Wo sind die größten Risiken, was müssen wir tun?
- ISB generiert Bericht A.5 mit 4000 Seiten
- Kunde hat jetzt einen anderen ISB

Grundschutz nach 200-2

Top-Down-Ansatz

- Sinnvoll, wenn Management „mitspielt“
- Was brauchen wir, damit unsere Organisation ihren Zweck erfüllt?
- Großzügige Gruppierungen
- Strategie: Schnell hier durch, dabei das Wesentliche erfassen!
- Vorgehensweise: Kern-Absicherung

Bottom-Up-Ansatz

- Strukturanalyse, Modellierung
  - Organigramm abbilden
  - Geschäftsprozess = Verarbeitungstätigkeit
  - Großzügige Gruppierungen
- Grundschutz-Check
  - Basis-Absicherung
- Risikoanalyse?
  - Später, wenn wir mal Zeit haben…

Risikoanalyse nach 200-3

Zweckmäßige Risikomatrix

- Matrix später ändern?

⇒ alle Risikoanalysen müssten wiederholt werden!

- Abgleich mit Unternehmens-Risikomanagement (wenn möglich)
- Eintrittswahrscheinlichkeit 10%, 40%, 70%

  - pro Monat, pro Jahr oder was ???

- Logarithmische Skalen nutzen!
- Schadensklassen sollten mit Schutzbedarfsdefinitionen abgestimmt sein

Risikokategorie

Sehr hoch	Die umgesetzten Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Sehr hohe Risiken werden nicht akzeptiert.
Hoch	Die umgesetzten Sicherheitsmaßnahmen bieten keinen ausreichenden Schutz vor der jeweiligen Gefährdung. Ein hohes Risiko kann nur von der Leitungsebene nur zeitweise, oder wenn alle Maßnahmen zur Verringerung des Risikos ausgeschöpft wurden, akzeptiert werden.
Mittel	Die umgesetzten Sicherheitsmaßnahmen reichen möglicherweise nicht aus. Das Risiko wird implizit akzeptiert, beobachtet und an die Leitungsebene berichtet.
Gering	Die umgesetzten Sicherheitsmaßnahmen bieten einen ausreichenden Schutz. Das Risiko wird implizit akzeptiert.

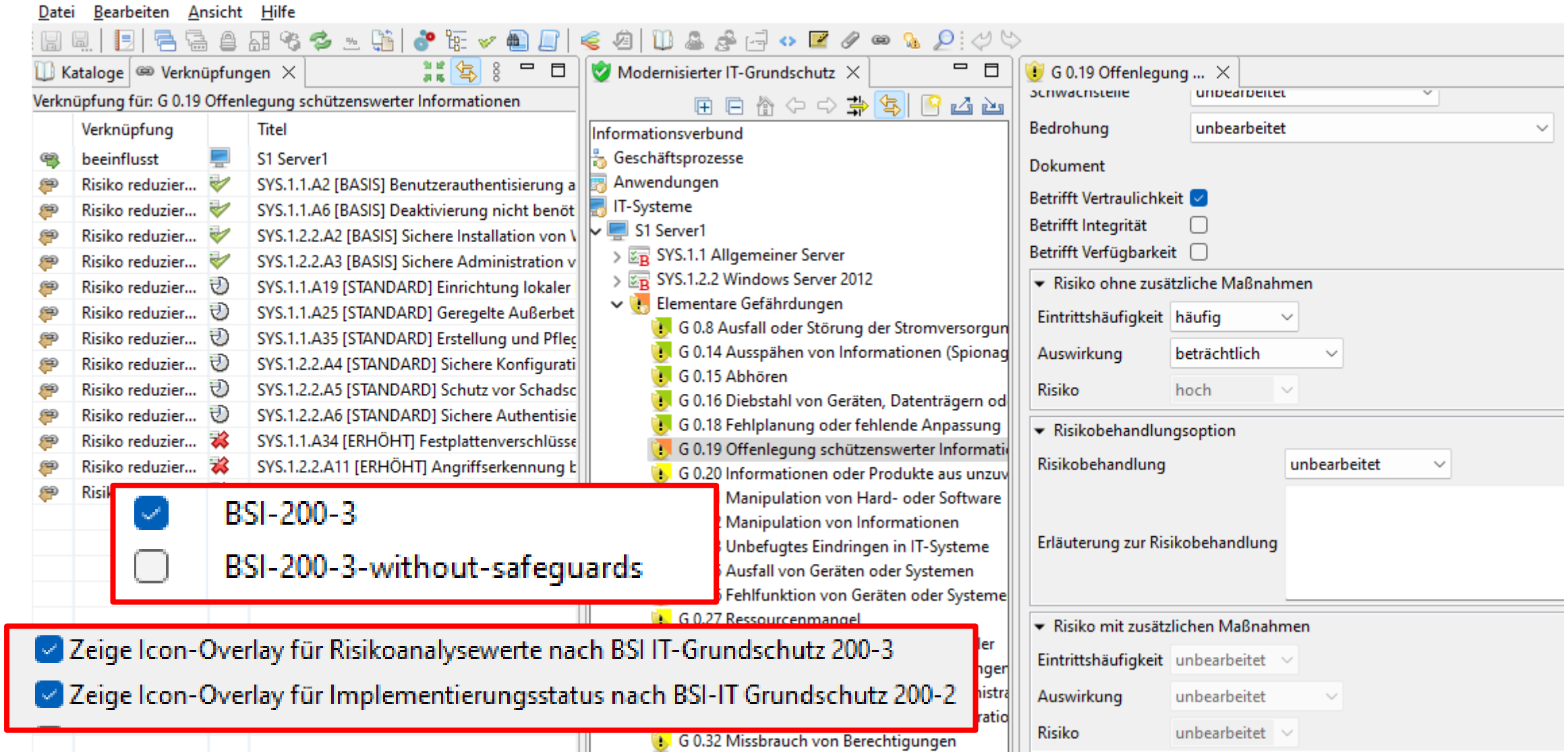
existenzbedrohend	mittel	hoch	sehr hoch	sehr hoch
beträchtlich	mittel	mittel	hoch	sehr hoch
begrenzt	gering	gering	mittel	hoch
vernachlässigbar	gering	gering	gering	gering
	5 J	1 J	1 M	

5 Mio €	mittel	hoch	sehr hoch	sehr hoch	sehr hoch
500 T €	gering	mittel	hoch	sehr hoch	sehr hoch
50 T €	gering	gering	mittel	hoch	sehr hoch
5 T €	gering	gering	gering	mittel	hoch
	gering	gering	gering	gering	mittel
	100 J	10 J	1 J	1 M	

Durchführung der Risikoanalyse

- Workshop mit Informationseigentümer (Schadenshöhe), Admin (Eintrittswahrscheinlichkeit), ISB/Berater (Moderation)
- Aufwand: 1 bis 2 Stunden pro Zielobjekt
- Priorisierung:
  - Erhöhter Schutzbedarf
  - Fehlende Grundschutz-Bausteine
  - Maßnahmen nicht umgesetzt
  - Ad-Hoc für „schwierige Fragen“

Verinice-Einstellungen



Ergebnis der Risikoanalyse

- Möglichst keine „sehr hohen“ Risiken
- Zweistellige Anzahl „hoher“ Risiken, muss vor Umsetzungsplanung konsolidiert werden
- Risiken sind zu behandeln, wenn sie erkannt werden – nicht wenn alle Risikoanalysen abgeschlossen wurden

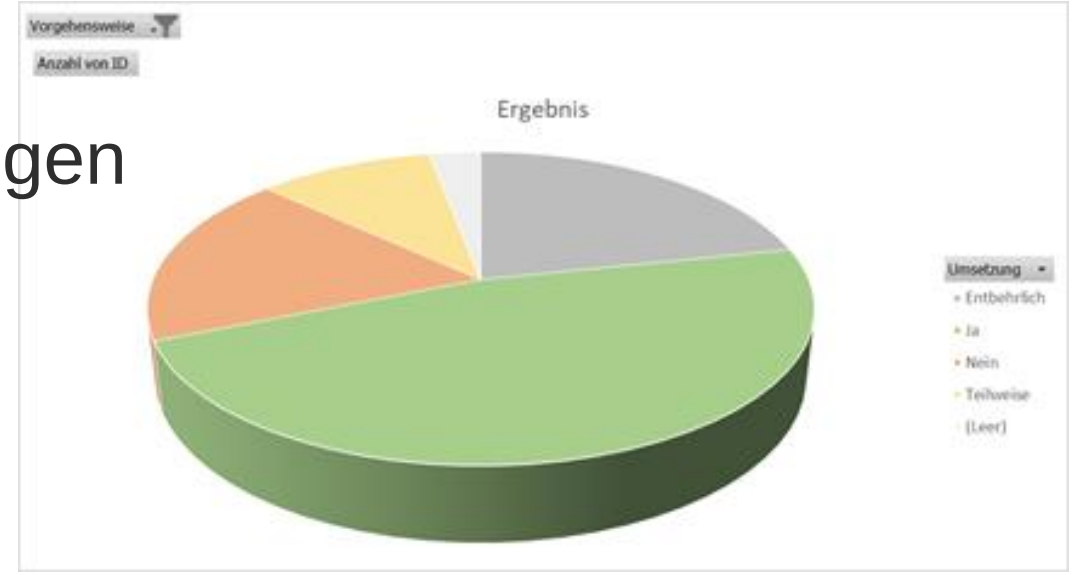
Management-Report

Gehe oft zu Deinem Fürst, auch wenn Du nicht gerufen wirst…

- ISB ist Stabsstelle!
- Regelmäßige Reports
  - quartalsweise bis jährlich
- Anlassbezogene Reports
  - schwerwiegende Sicherheitsvorfälle
  - erkannte sehr hohe Risiken
  - aktuelle Ereignisse
    („Kann uns das auch passieren?“)

Bericht Grundschutz-Umsetzung

- Report-Abfragen auf alle Schichten
  - In Excel importieren, Pivot-Tabelle, Diagramm
- Umsetzung BASIS-Anforderungen
  - nicht umgesetzte BASIS-Anforderungen grenzen an grobe Fahrlässigkeit
- Umsetzung STANDARD-Anforderungen
  - Hinweis auf „Stand der Technik“



Bericht über Informationssicherheit-Risiken

- Ein Risiko „Sehr hoch“ ist wie ein Sicherheitsvorfall zu behandeln
- Jedes Risiko „Hoch“ wird einzeln berichtet
- Risiken „Mittel“ und „Gering“ werden summarisch berichtet

Makrosicherheit			
Wahrscheinlichkeit	Schadensausmaß	Risiko	Risikobehandlung
Häufig	Hoch	Hoch	Reduktion

Schadsoftware tarnt sich sehr häufig als Office-Makro. Die eingesetzten Virenscanner erkennen nicht jede Schadsoftware, eine nicht erkannte und ausgeführte Schadsoftware würde einen hohen Schaden verursachen.
Empfehlung:
Stand der Technik ist es, Makros generell zu deaktivieren und nur per Whitelisting zu aktivieren. Derzeit ist nicht bekannt, inwieweit Makros in Fachverfahren benötigt werden. Der Einsatz von Makros in Fachverfahren sollte analysiert werden. Benötigte Makros müssen entweder über Pfade oder über digitale Signatur ins Whitelisting aufgenommen werden. Anschließend muss die Ausführung von anderen Makros generell gesperrt werden.

Umsetzungsplanung

- Handlungsoptionen für jedes Risiko „Hoch“ ermitteln
- Aufwandsschätzung durch Fachabteilung für jede Handlungsoption „Risikoreduktion“
- Entscheidungsvorlagen erstellen
- Management-Entscheidung dokumentieren
- Projekt / Change initiieren
- Umsetzung dokumentieren: Das Risiko „verschwindet“ erst mit der Fertigstellung des Projektes / Changes.

Fragen?

ulf@riechen.consulting

+49 170 2467199