ISMS in einem Landratsamt

die Balance zwischen begrenzten Ressourcen, dem Wunsch nach korrektem Verwaltungshandeln und angemessener Sicherheit

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

Agenda

Anforderungen

Ausgangszustand

Schutzbedarf

Grundschutz-Vorgehensweise

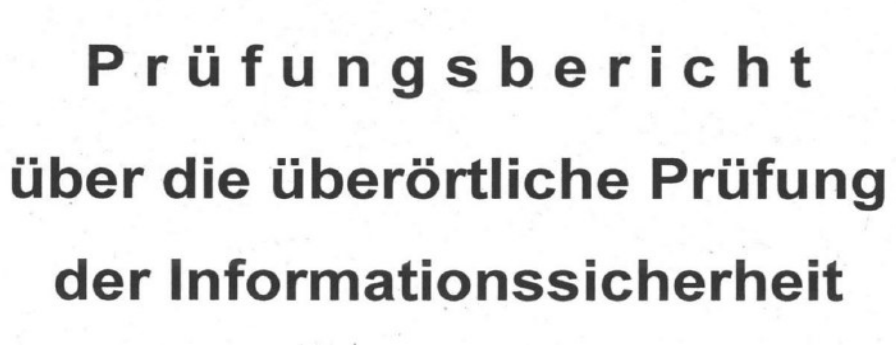
Reporting

Fazit

Anforderungen

Anforderungen

- EU-Zahlstelle
  - „Outsourcing-Dienstleister“ für BSI-zertifiziertes SMUL
- Waffenregister
  - Vorgabe: Grundschutz + Prüffragen
- Rechnungshof



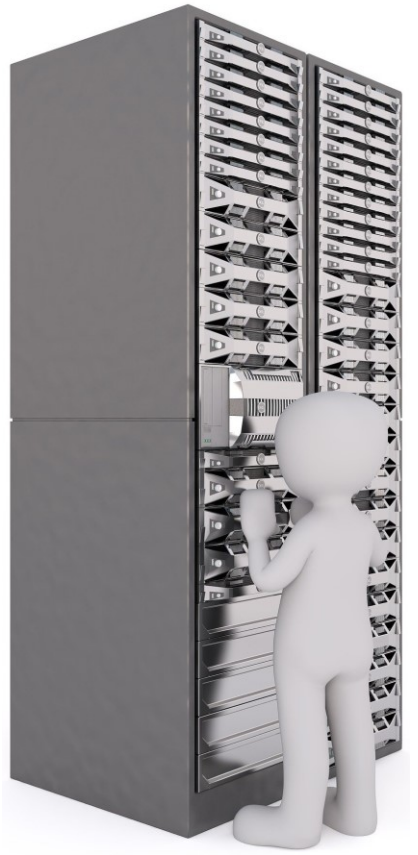
Die Ermittlung des Schutzbedarfes sollte deshalb vorrangig bearbeitet werden.

4.3.2.2 Regelungen zur Schutzbedarfsfeststellung

Die Vorgehensweise zur Schutzbedarfsfeststellung war nur in 4 Landkreisverwaltungen explizit geregelt, wobei aber in einer Landkreisverwaltung der Schutzbedarf nur für die Verfahren ELER und Nationales Waffenregister durchgeführt wurden. In einer Landkreisverwaltung gab es zumindest den Entwurf einer Richtlinie. Eine Landkreisverwaltung hat Schutzbedarfsfeststellungen ohne Regelungen durchgeführt, lediglich per Hausmitteilung an die Fachbereiche die Feststellung des Schutzbedarfs erläutert und ein Formular beigefügt. Zwei weitere Landkreisverwaltungen haben den Schutzbedarf ohne entsprechende Regelungen zumindest für die Verfahren ELER oder Nationales Waffenregister festgelegt.

Ausgangszustand

Zustand der Informationssicherheit



- IT-Sicherheit?
  Das macht das Sachgebiet EDV im Hauptamt.
- Redundanzen? Haben wir!
  - Zwei Blade-Center mit VMware HA und zwei NetApps
  - … 4 Meter voneinander entfernt
  - … im gleichen Serverraum
  - … im Keller
  - … jetzt mit Pumpe (nach dem letzten Wassereinbruch)
- Nutzer werden nach 3 Passwort-Fehleingaben dauerhaft gesperrt.

Zustand der Informationssicherheit

- Die Daten inaktiver Nutzer werden nach 6 Wochen gelöscht.
- Sicherheitspatches spielen wir ein!
  - … wenn wir Zeit haben
  - … aber nicht auf den kritischen Fachverfahren
  - … und nicht auf den Servern mit Windows 2003
- Nanu, ich kann mich nicht mehr anmelden?
  - Ja, Sie wurden deaktiviert. Alle Dienstleister werden jede Nacht deaktiviert. Wenden Sie Sich an den Benutzerservice!
  - … 30 Minuten später bin ich wieder arbeitsfähig.
  - Das gleiche Spiel zu Beginn jedes Projekttages…

Zustand der Notfallvorsorge

- Notfallmanagement macht der Kreisbrandmeister.
  - … im Krisenstabsraum
  - … mit Desktop-PC
- IT-Ausfall
  - … darf im Katastrophenfall nicht passieren!

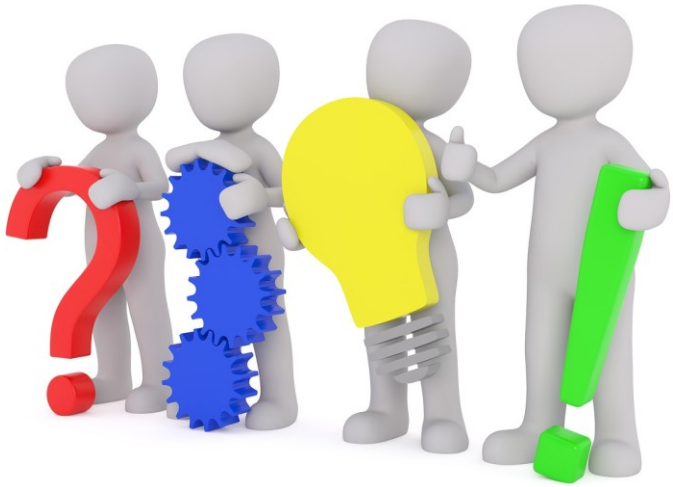
Schutzbedarf

Kick-Off-Workshop

- 90 Minuten mit Referatsleitern
- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Notfallvorsorge

Schutzbedarfskategorien

- Schadenshöhe
  - 1 – unkritisch, 2 – mittel, 3 – hoch, 4 – sehr hoch
- Szenarien
  - Finanzieller Schaden
  - Beeinträchtigung der Aufgabenerfüllung
  - Verstoß gegen Gesetze oder Verträge
  - Image-Schaden
  - Gefahr für Leb und Leben
  - Datenschutz



Auswirkung	Schadensszenario „Beeinträchtigung des informationellen Selbstbestimmungsrechts“ Wie beeinträchtigt ein Sicherheitsvorfall den Schutz personenbezogener Daten?
1 - unkritisch	Eine Beeinträchtigung erscheint nicht möglich.
2 - mittel	Es ist mit einer tolerierbaren Beeinträchtigung der gesellschaftlichen Stellung bzw. der wirtschaftlichen Verhältnisse Betroffener (typischerweise überschaubarer finanzieller Verlust bzw. Ansehensverlust) zu rechnen.
3 – hoch	Es ist mit einer erheblichen, jedoch keiner existenzbedrohenden Beeinträchtigung der gesellschaftlichen Stellung bzw. mit einer Gefährdung der wirtschaftlichen Existenz Betroffener (typischerweise: Insolvenz) zu rechnen.
4 – sehr hoch	Es ist mit einer existenzbedrohenden Beeinträchtigung der persönlichen Freiheit Betroffener (typischerweise: Gefahr für Leib und Leben) zu rechnen.

Erhebungsbogen

- Vertraulichkeit, Integrität
  - Je Szenario
  - Mit Begründung
- Verfügbarkeit
  - Je Szenario
  - Mit Begründung
  - Ab wann welcher Schaden?
  - Service-Zeiten, Aufbewahrungsfristen
- Not-Arbeitsplätze
  - Ab wann, wer, welche Technik, welche Daten, … (analog UMRA)

Betriebszeiten		Bemerkungen
Regelmäßige Betriebszeiten	24x7	Nachts laufen automatische Prozesse
Aufbewahrungsfristen für Daten	10 Jahre	Archivgesetz für den Freistaat Sachsen

Schadensszenario	< 4 h	< 24 h	< 3 d	< 10 d	> 10 d
Finanzielle Auswirkungen	1	1	2	3	3
Begründung der Bewertung	Ab 3 Tagen Ausfall erstehen Schäden von mehr als 500 T€, da Verzugszinsen und Mahngebühren anfallen.				
Beeinträchtigung der Aufgabenerfüllung	2	2	2	2	3
Begründung der Bewertung	Ab 10 Tagen Ausfall können die aufgelaufenen Daten nicht mehr durch eigenes Personal erfasst werden.				

Grundschutz-Vorgehensweise

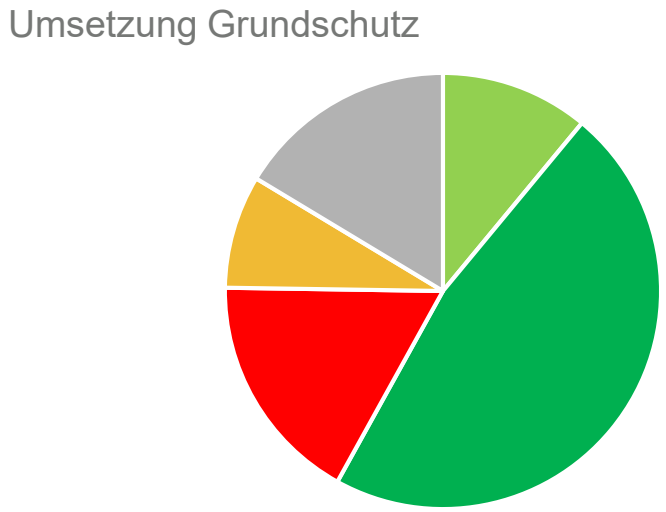
Grundschutz-Vorgehensweise

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

Reporting

Reporting

- Projekt-Bericht
  - Schutzbedarf/BIA
  - Risiken
- Quartals-Bericht ISB
  - Stand der Informationssicherheit
  - Risiken incl. Vorschläge zum Umgang mit Risiken
  - Planungen zu Sicherheitsmaßnahmen



Fazit

Erfahrungen aus Projekten in der öffentlichen Verwaltung

- Der Dienstweg ähnelt dem Spiel „Stille Post“.
  - Informationssicherheit braucht direkte Wege (IS-Management-Team).
- Qualität heißt:
  - Das Produkt erfüllt seinen Zweck.
  - Ungefähr richtig ist besser als gar nicht.
  - Wir machen das erstmal so. Und wenn es sich nicht bewährt, dann verbessern wir es (PDCA).

Fragen?

ulf@riechen.consulting

+49 170 2467199