LF4 Klausur zum Thema "Schutzbedarfsanalyse"

Nico Schädlich, 25.11.2024 Kontakt: nico@schulenimchaos.de

Schutzbedarfsanalyse

Was sind die BSI-Standards?

Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik.

Was bedeuten die Standards "BSI 100-1, 100-2, 100-3"?

Veraltete aber dennoch gängige Standards.

- 100-1 beschreibt grundlegende Anforderungen an ein ISMS (InformationsSicherheit-ManagementSystem) und welche Aufgaben es bewältigen muss.
- 100-2 beschreibt einen Weg, diese Anforderungen umzusetzen.
- 100-3 beschreibt eine vereinfachte Risikoanalysemethodik.

Gefährdungs-, Maßnahmen-, Bausteinkatalog?

- Im Gefährdungskatalog sind mögliche, verbreitete Gefährdungen gelistet.
- Im Maßnahmenkatalog Maßnahmen, um genau diese Gefährdungen zu bekämpfen.
- Im Bausteinkatalog ist aufgelistet, wer welche Aufgabe hat, um die Maßnahmen umzusetzen.

Warum müssen sich Unternehmen vor möglichen Gefährdungen schützen?

- Das Unternehmen trägt die volle Verantwortung für sensible Daten, welche u.a. für die Zukunft des Unternehmens von hoher Bedeutung sein können.
- Mögliche Gefährdungen / Verstöße der DSGVO werden sehr hoch bestraft, hierdurch werden also möglicherweise hohe Kosten verhindert.

Wie sieht der Sicherheitsprozess in einem Unternehmen aus?

Es wird oftmals nach dem PDCA-Modell gearbeitet.

- P(lan): Es wird geplant, welche Maßnahmen konkret ergriffen werden sollen.
- D(o): Es werden entsprechende Maßnahmen umgesetzt.
- C(heck): Es wird überprüft, ob die Implementierung erfolgreich war oder nicht.
- A(ct): Die implementierten Maßnahmen werden optimiert und verbessert.

So ist ein kontinuierlicher Prozess gegeben, der dauerhaft und nachhaltig für eine Verbesserung der IT-Sicherheit im Unternehmen sorgt und eine (im Verhältnis) zeitnahe Umsetzung von gesetzlichen Anforderungen ermöglicht.

Mängel im Management, die im Weg stehen können

In der Regel entstehen bei der Umsetzung immer Probleme. Mögliche Probleme hier sind zum Beispiel:

- fehlende persönliche Verantwortung schlechte Konzepte
- zu wenig oder fehlgeleitete Investitionen
- keine Aktualisierung im Sicherheitsprozess
- keine Durchsetzbarkeit von Maßnahmen

Gelöst werden diese Probleme meist relativ einfach, in dem man für die nötige Kompetenz sorgt, die nötigen Befugnisse einräumt und natürlich auch den nötigen Handlungsspielraum zulässt. Gleichzeitig sollte sich ein Geschäftsführer immer selbst in der Verantwortung, die Sicherheit im Unternehmen zu gewährleisten, sehen.

Ab einer bestimmten Größe empfiehlt es sich, einen IT-Sicherheitsbeauftragten (ISB) zu ernennen.

Was macht ein ISB?

Ein ISB lenkt den Sicherheitsprozess, koordiniert die Implementierung von neuen Sicherheitskonzepten, leitet Untersuchungen von relevanten Vorfällen und kümmert sich um die Schulung von Mitarbeitern.

Was ist eine Sicherheitsleitlinie?

In einer Sicherheitsleitlinie soll verständlich beschrieben werden, welche Ziele angestrebt werden und mit welchen Mitteln sie umgesetzt werden sollen. Dabei werden außerdem Geltungsbereiche und Organisationsstrukturen berücksichtigt.

Was ist ein Sicherheitskonzept?

Mit einem Sicherheitskonzept werden die in der Leitlinie festgelegten Ziele konkret mit Strategien zur Implementierung verbunden.

1. Strukturanalyse: Erfassen der Komponenten eines Informationsverbundes
2. Schutzbedarfsfeststellung: Bedarf an Vertraulichkeit, Verfügbarkeit und Integrität bestimmen
3. Maßnahmenbestimmung: Passende IT-Grundschutz-Bausteine auswählen und Soll-Zustand mit Ist-Zustand vergleichen
4. Sicherheitsanalyse: Prüfen ob noch mehr Sicherheit gebraucht wird, und wenn ja: durch welche Risiken
5. Konsolidierung: Alle erfassten Maßnahmen zusammenführen
6. Umsetzung der Maßnahmen prüfen
7. Maßnahmen technisch und organisatorisch umsetzen

Was ist eine "Strukturanalyse"?

Wie der Name bereits sagt, wird die Struktur eines Netzwerks analysiert, sprich physische (räumliche) Komponenten wie Serverräume, aber auch logische Komponenten wie Anwendungen, werden erfasst und zusammengetragen, um Abhängigkeiten aufzudecken.

Wie läuft eine Strukturanalyse ab?

1. Informationen, Geschäftsprozesse, Abläufe erheben
2. Logischen Netzplan erstellen
3. IT-Systeme erfassen (Clients, Server, Switches, etc.)
4. räumlichen Begebenheiten (wo stehen die Clients, Server und Switches) erfassen