SiKoSH
SICHERHEIT FÜR KOMMUNEN
IN SCHLESWIG-HOLSTEIN

SiKoSH Handreichung
Anleitung – Bearbeitung der SiKoSH Quickcheckphasen

Version:	1.0.0
Datum:	14.10.2017
Kontakt:	KomFIT e.V. Kiel sikosh@komfit.de https://www.sikosh.de

Vorraussetzungen

Zur Nutzung der Quickchecks wird Microsoft Excel ab Version 2003 oder ein kompatibles Programm benötigt.

Beschreibung der Registerkarten

- Quickcheck <Quickcheckname>
  - Diese Registrierkarte beinhaltet den eigentlichen Quickcheck
- Darstellung der Erfüllung
  - Diese Registrierkarte beinhaltet eine einfache grafische Übersicht (Kuchendiagramm usw.)
- Hilfstabelle
  - Diese Registrierkarte beinhaltet Hilfsformeln. Für den Bearbeiter der Quickches ist sie irrelevant.
- Notizen
  - Diese Registrierkarte beinhaltet verweiße auf IT-Grundschutzmaßnahmen zur ergänzenden Information und weiterführenden Bearbeitung der Quickchecks.

Beschreibung der Spaltenüberschriften

- Nr.
  - Diese Spalte beinhaltet die laufende Nummer der Prüffrage
- Frage
  - Diese Spalte beinhaltet eine recht umfassende Prüffrage, deren Beantwortung sich durch einen Abgleich mit den einzelnen Prüfpunkten ergibt.
- Punkt
  - Diese Spalte beinhaltet die die forlaufende Nummerierung der einzelnen (Sub-) Prüfpunkte.
- Prüfpunkte
  - Diese Spalte beinhaltet einen SOLL – Sachverhalt, der so in der anwendenden Institution umgesetzt sein sollte.
- Priorität
  - Diese Spalte beinhaltet einen Vorschlag hinsichtlich der Wichtigkeit (Hoch, Normal, Niedrig, Optional) des Prüfpunktes im Hinblick auf das ganzheitliche Sicherheitsniveau der umsetzenden Institution. „Optional“ wurde immer dann gewählt, wenn ein solcher Punkt nur unter bestimmten Umständen vorkommt (z.B. ist eine geeignete Vertragsgestaltung mit einem externen IT-Sicherheitsbeauftragten auch nur dann vorzunehmen, wenn tatsächlich ein externer IT-Sicherheitsbeauftragter bestellt wurde und die Besetzung der Rolle nicht mit internen Ressourcen abgebildet wird).
  - Ein Prioritätsvorschlag ist in jedem Quickcheck enthalten. Der Anwender mag aber im Einzelfall die Priorität auf die tatsächlichen individuellen Gegebenheiten seiner Organisation anpassen.
- Bewertung
  - Hier hat der Anwender die Möglichkeit den Erfüllungsgrad der einzelnen Prüfpunkte innerhalb seiner Institution zu dokumentieren. Er kann hier zwischen den Abstufungen „Vollständig erfüllt“, „Fast erfüllt“, „Teilweise erfüllt“, und „Nicht erfüllt“ wählen. Der Umsetzungsgrad „Nicht anwendbar (Entfällt)“, ist vergleichbar mit dem aus dem IT-Grundschutz bekannten „Entbehrlich“. Daher können

Prüfpunkte die auf die individuelle Gegebenheiten der Institution nicht anwendbar sind, entsprechend markiert werden.

- Notizen
    - Hier können eigene Notizen während der Bearbeitung der Quickchecks hinterlegt werden.

Allgemeine Hinweise und Zielsetzungen

Die Bearbeitung der SiKoSH Quickchecks stellt eine stark vereinfachte Form eines Basis-Sicherheitschecks (ohne vorherige Strukturanalyse bzw. Modellierungsphase) gemäß der IT-Grundschutzvorgehensweise des BSI dar. Damit sind diese zwar einfacher anwendbar, bieten aber andererseits nicht den Umfang und Detailierungsgrad eines Basissicherheitschecks nach der IT-Grundschutzvorgehensweise.

Der SiKoSH Standard und weitere Hilfsmittel

Im SiKoSH-Standard „Vorgehensweise zur Einführung eines ISMS nach SiKoSH“ werden die einzelnen Phasen und die Reihenfolge der Bearbeitung der Quickchecks erläutert. Dazu wird innerhalb des Standards zu jeder Quickcheckphase, auf jeweils geeignete Hilfsmittel mit Vorlagencharakter zur individuellen Anpassung verwiesen. Diese Hilfsmittel ermöglichen eine einfachere Implementierung notwendiger Sicherheitsprozesse und Dokumentationen innerhalb der anwendenden Institution.

Vorgehen bei der Bearbeitung der SiKoSH Quickchecks

Wie auch im SiKoSH-Standard „Vorgehensweise zur Einführung eines ISMS nach SiKoSH“ weiter erläutert, sollten SiKoSH Anwender wenigsten, frei nach dem Pareto-Prinzip, wenigsten 80% der im jeweiligen Quickcheck aufgeführten Prüfpunkte dokumentieren und, falls notwendig, initiieren.

Sollte also die Bewertung der Erfüllung eines Prüfpunktes nur ein „Teilweise erfüllt“ oder „Nicht erfüllt“ ergeben, sind in der Regel weitere Aktionen erforderlich um geeigente Maßnahmen auf den Weg zu bringen.

Als Beispiel soll an dieser Stelle der Prüfpunkt „Eine ISMS Leitlinie wurde erstellt und durch die Insititutionsleitung unterschrieben und in Kraft gesetzt.“ genannt werden. Hier sollte das entsprechende Hilfsmittel auf die individuellen Gegebenheiten der anwendenden Institution angepasst werden, bevor der nächste Quickcheck bearbeitet wird. Allerdings ist es nicht erforderlich, Abstimmungsphasen und die formale Unterschrift der Institutionsleitung abzuwarten, bevor mit der Bearbeitung des nächsten Quickchecks begonnen werden kann.