IT-Grundschutz Konzept nach BSI für die Curaden AG

Themenbereiche:	ICT Business Solutions, ICT Infrastrukturen, Security/Privacy
Studierende:	Brunner Dominik, BSc Wirtschaftsinformatik (WI)
Betreuungsperson:	Oliver Hirschi
Experte:	Yves Kraft
Auftraggebende:	Tobias Bernet, Curaden AG
Keywords:	Informationssicherheit, ISMS, Reifegrad, BSI, ISO 27001, NIST

1. Aufgabenstellung

Die Curaden AG als Auftraggeber dieser Arbeit ist ein international tätiges Unternehmen im Dentalhygiene und -medizin Bereich mit Vertrieb in über 72 Ländern. Das Unternehmen ist in den letzten Jahrzehnten unter anderem dank seiner hohen Anpassungsfähigkeit stetig gewachsen und beschäftig heute schweizweit circa 200 Mitarbeitende an zehn Standorten. Diese schnelle Entwicklung verbunden mit einigen personellen Änderungen in der IT-Leitung haben dazu geführt, dass die Anliegen der Informationssicherheit meist nur punktuell und technisch adressiert werden konnten.

Ziel der Bachelorarbeit ist es, durch den Einsatz der BSI IT-Grundschutz Standards eine Übersicht über die aktuelle Informationssicherheitslage der Curaden AG zu bekommen. Zusätzlich sollen für ausgewählte, nicht oder nur teilweise erfüllte Sicherheitsanforderungen Massnahmenempfehlungen ausgearbeitet werden. Die Erkenntnisse aus beiden Phasen können dann für die Verbesserung der Informationssicherheit im Unternehmen eingesetzt werden.

2. Lösungskonzept

Um nützliche Hinweise für die Einführung eines Information Security Management System (ISMS) zu gewinnen, wurde zuerst eine Auslegung des BSI Grundschutzes gemacht und mit dem Vorgehen des ISO 27001 verglichen. Anschliessend wurde ein Interview mit einem für Informationssicherheit verantwortlichen CIO eines Unternehmens aus der Zentralschweiz gemacht, um von den ISMS Erfahrungen eines vergleichbaren, aber grösseren Unternehmens zu profitieren. Zusätzlich wurde ein Interview mit einem Security Experten der Bithawk AG gemacht, um dessen Inputs ebenfalls in die bevorstehe ISMS-Einführung bei der Curaden aufzunehmen.

Zum Start der Umsetzung wurden ein Interview mit der IT-Leitung durchgeführt, um Grundlageinformationen für die Erstellung der Sicherheitsleitlinie und des Sicherheitskonzeptes zu erlangen. Diese Informationen wurden dann zum einen genutzt, um Vorschläge und Empfehlungen für den Aufbau des organisatorischen Rahmens zu erstellen, welche für das ISMS vorausgesetzt werden. Zum anderen konnte damit bereits ein erster IT-Grundschutz Check durchgeführt werden, um die aktuelle Informationssicherheitslage bei den Core-Systemen überblicken zu können.

Zum Schluss wurden dann einige ausgewählte Anforderungen, welche nicht oder nur teilweise erfüllt waren, mit ausgearbeiteten Massnahmenempfehlungen adressiert.

3. Spezielle Herausforderungen

Die Suche nach Praxiserfahrungen zur Einführung eines ISMS in einem KMU stellte sich als schwierig heraus, weil die Unternehmen es vermeiden, jegliche Informationen zu Themen der IT-Sicherheit oder der Informationssicherheit gegen aussen dringen zu lassen.

Auch die konzeptionelle Umsetzung der ISMS Einführung für die Curaden war eine Herausforderung, denn es fehlte auf der einen Seite an den Voraussetzungen für eine ISMS Einführung nach BSI IT-Grundschutz, wie zum Beispiel der Awareness der Geschäftsleitung oder eine Übersicht der gesetzlichen Verpflichtungen der Firma. Zudem mangelte es an Dokumentationen, um bei der Strukturanalyse, Geschäftsprozesse, Anwendungen und IT-Systeme analysieren und festhalten zu können.

4. Ergebnisse

Im Rahmen der Bachelorarbeit wurden folgende Ergebnisse erarbeitet:

- Vorschläge und Empfehlungen für den Aufbau des organisatorischen Rahmens eines ISMS
- Eine tabellarische Auflistung der relevanten Sicherheitsanforderungen an den Informationsverbund der wichtigsten Geschäftsprozesse mit dem jeweiligen Erfüllungsgrad
- Fünf Massnahmenempfehlungen zu nicht erfüllten Sicherheitsanforderungen

Diese Ergebnisse dienen als Hilfestellungen für eine schrittweise Einführung eines ISMS.

5. Ausblick

Mit dieser Bachelorarbeit ist nur ein kleiner Schritt in die Richtung einer Einführung eines funktionierenden ISMS gemacht worden. Mit Hilfe der hier gemachten Vorschläge und Empfehlungen können die organisatorischen Grundlagen für die Informationssicherheitsprozesse geschaffen werden. Dies beinhaltet als Erstes den Aufbau eines Informationssicherheitsbeauftragten (ISB), die Zuteilung der nötigen Ressourcen und die Definition des Informationssicherheitsteams. Danach muss eine Sicherheitsrichtline erstellt und publiziert werden, welche den Mitarbeitenden den Stellenwert und die Absichten der Informationssicherheit verständlich machen kann.

Parallel dazu kann mit Hilfe der Sicherheitsanforderungen und den konkreten Massnahmenempfehlungen bereits an einer Härtung des Informationsverbunds gearbeitet werden.

Sobald die Grundlagen geschaffen wurden, kann der ISB anfangen die Informationssicherheitsprozesse iterativ weiterzuführen.