**Zusammenfassung/Abstract Semesterarbeit**

**Audit-Methode zur Gefahrenanalyse einer KMU IT-Infrastruktur**

**Einleitung**

Grundlage dieser Semesterarbeit ist ein Projekt, das von der ZHAW zusammen mit einem Industriepartner durchgeführt wird. Ziel des Projektes ist die Entwicklung einer generischen Audit-Methode zur Gefahren- und Risikoberechnung. Diese Methode ist konzeptionell soweit ausgereift, dass damit erste Praxiserfahrungen gesammelt werden können. In dieser Semesterarbeit soll die bereits entwickelte Methode so angepasst werden, dass es möglich ist, Gefahren einer IT-Infrastruktur aufzuzeigen. Zusätzlich soll ein Prototyp erstellt werden, mit dem die Methode angewendet werden kann.

**Arbeit**

In einem ersten Schritt wurde die Methodik formell beschrieben. Jedes Element konnte nun mit einer Variabel beschrieben und alle Berechnungen durch eine Gleichung ausgedrückt werden.

Als nächstes mussten die generischen Teile der Methode, die Prüfungskriterien sowie die Attribute, die Schäden beschreiben, an die IT Branche angepasst werden. Zu deren Bestimmung wurde der *ISO/IEC 27002:2005* Standard, der *Leitfaden Informationssicherheit* des BSI sowie diverse IT-Security-Audits verwendet. Dadurch entstand eine Liste von 59 Prüfungskriterien. Als schadensbeschreibende Attribute wurden *Verfügbarkeit*, *Integrität* und *Vertraulichkeit* definiert.

Mit diesen, in den ersten zwei Arbeitsschritten erarbeiteten Grundlagen konnte der Prototyp erstellt werden. Wichtig bei der Entwicklung war, dass der Prototyp die Methode anschaulich darstellen lässt und möglichst einfach zu gebrauchen sowie zu installieren sein muss. Deshalb wurde er als HTML5 Web-Applikation umgesetzt. Die einzige Voraussetzung um den Prototyp zu verwenden, ist somit ein moderner Web-Browser.

Beim abschliessenden Test des Prototyps auf Funktionalität und Anwendbarkeit zeigte sich, dass die Funktionalität erfüllt war, die Anwendbarkeit jedoch einige Schwächen aufwies: Die Formulierung der Prüfungskriterien sowie der Bewertungsmöglichkeiten. Diese wurden angepasst.

**Fazit**

Alle Aufgaben konnten erfüllt und die Semesterarbeit somit abgeschlossen werden. Um die Methode abschliessend an die IT-Branche anzupassen bräuchte es jedoch die Mitarbeit mehrerer IT-Security-Experten, welche die Relevanz und Korrektheit der Liste der Prüfungskriterien, der Attribute sowie deren Bewertung sicherstellt. Mit dem Prototyp kann die Methode angewendet werden, jedoch erlaubt er nur das Ausfüllen eines einzigen Audits. Wollte man die Methode professionell anwenden, würde es sich anbieten, eine Web-Applikation mit einer Datenbank im Hintergrund zu entwickeln. Dies würde eine Auswertung vorgenommener Audits erlauben, mit welcher man einen Einblick in die Sicherheitslage der Schweizer KMUs erhalten könnte.