

IT Sicherheits Ausgaben, Priorisieren & Optimieren

Zu diesen Thema werden die unterschiedlichsten Behauptungen veröffentlicht. Diese Ausführungen sollen zur Klärung beitragen.

RISIKO

Sicherheit bedeutet auch Risiko-Management. Das heisst die Risiken zu erkennen und zu evaluieren um sie entweder zu akzeptieren, durch entsprechende Massnahmen zu mindern oder zu versichern. Dieser Prozess wie auch die Entscheidung soll nachvollziehbar sein. Dementsprechend ist der Prozess zu dokumentieren und zu kommunizieren.

Wenn Geld für solche Massnahmen ausgegeben wird, als Investition oder Betriebskosten, so wird eine Risiko-Minderung angestrebt. Diese Risiko-Minderung soll in einem vertretbaren Verhältnis zu den Ausgaben stehen. Soweit sind wir uns alle einig.

ROSI

Wenn man nun versucht, die Grösse "Risiko-Minderung" in Franken auszudrücken um eine Kosten-Nutzen Rechnung zu erstellen, so heisst dieses Verfahren **ROSI** "Return On Security Investment."

Diese Aussage von ROSI hat sehr viel Potential; Doch ist es leider nicht immer möglich, Risiken mit gesicherten Werten zu quantifizieren. Risiken sind "erwartete Schäden", das heisst das Produkt aus Schadensausmass und Eintretenswahrscheinlichkeit (oder für Wahrscheinlichkeits-Puristen) Schadensausmass x Häufigkeit).

Bei Ereignissen, welche mehrmals pro Jahr eintreten, können wir auf Erfahrungswerte zurückgreifen, welche uns einigermaßen vertrauenswürdige und genaue Zahlen für die Eintretenswahrscheinlichkeit sowie das Schadensausmass liefern.

Dagegen sind für grosse Schadensereignisse (Katastrophen), welche nur alle 20, 50 oder 100 Jahre erwartet werden, sowohl die Eintretenswahrscheinlichkeit als auch das Schadensausmass ungewiss. Die Eintretenswahrscheinlichkeit lässt sich schlecht vorhersagen, weil wir die grundlegenden Mechanismen für solche Ereignisse weder verstehen noch aktuarische (versicherungsmathematische) Daten vorliegen haben. Der Schaden bei Katastrophenszenarien beinhaltet einen überwiegenden Anteil indirekter Kosten wie zum Beispiel Image-Schaden (Reputationsverlust) und dessen Folgekosten. Die Abschätzung dieser Kosten zeigt eine enorme Streuung welche zusammen mit der Ungewissheit über die Eintretenswahrscheinlichkeit eine ROSI Kalkulation für seltene Ereignisse unbrauchbar macht. Kuzum die Ergebnisse beinhalten zu viele Unsicherheiten und haben kaum Überzeugungskraft.

SORGFALTPFLICHT

Demgegenüber steht das andere Extrem inform der Aussage der Sorgfaltspflicht. Wir sollen gar nicht erst versuchen die Risiken zu messen, sondern unsere "Sorgfaltspflicht" (due care) zu erfüllen. Konkret bedeutet dies eine Anzahl (Baseline-) Massnahmen flächendeckend und allenfalls für besonders spezielle Fälle noch gezielt einzelne Sondermassnahmen zu implementieren. Wichtig ist, dass bei der Auswahl der Baseline-Massnahmen nur "Best-Practice" oder "Benchmarking" berücksichtigt wird (idealerweise aus der betreffenden Branche).

RISIKO-ANALYSE

In der IT Sicherheit wird generell empfohlen, sowohl mit Baseline-Massnahmen als auch mit Risiko-Analyse zu arbeiten. Risiko-Analyse in der Praxis heisst: Risiken zu kategorisieren (d.h. grob zu quantifizieren) und die grössten Risiken (High Risks) zu mindern oder bewusst zu akzeptieren. Eine detaillierte Risiko-Analyse ist enorm aufwendig und sollte nur in Ausnahmefällen angewandt werden.

Empfohlen wird ein mehrstufiges Verfahren. Dabei werden alle Projekte und Applikationen einer "Triage" unterzogen, um "besondere" Risiken, welche nicht durch die Baseline-Massnahmen abzudecken sind, zu identifizieren. Diese "Problemfälle" werden je nach Ergebnis einer "High-Level"- oder einer detaillierten Risiko-Analyse unterzogen. Bei der Auswahl der geeigneten Massnahmen um diese Risiken zu bewältigen, ist ROSI ideal.

Abschliessend bleibt zu sagen: IT Sicherheits-Ausgaben können und sollen, nicht nur auf Grund finanzieller Überlegungen getätigt werden, da wir nicht in der Lage sind alle Risiken ausreichend genau abzuschätzen.

Standards, "Best-Practices"- wie auch "Sorgfaltspflicht"-(Due-Care) Überlegungen sind berechtigt und bei seltenen Risiken notwendig.

Last but not least gilt es, die Gesetze, Richtlinien und Verträge (mit Lieferanten und Kunden) einzuhalten.