

# IT-Sicherheit kostet – ignoriert oder aktiv geführt

IT-Sicherheit ist kein Business Case – der propagierte «Return on Security Investment», kurz ROSI genannt, lässt grüssen. Investitionen in IT-Sicherheit sind der Preis, der für eine aktive Führung des Risikomanagements zu bezahlen ist. Markus Anton Meier



Markus Anton Meier  
ist Senior Consultant und Leiter  
der Technologiegruppe Security  
bei der AWK Group.  
markus.meier@awkgroup.com

Ist eine Firma nicht bereit, in ihre IT-Sicherheit zu investieren, dann spielt sie russisches Roulette. Wenn es gut geht, kommt sie ungeschoren davon, wenn ein «Worst Case» eintritt, überlebt sie unter Umständen nicht. Am Ende ist es eine Frage des Kerngeschäftes, des Umfeldes und des Risikoappetits oder der Ignoranz des Managements, ob und welche Anforderungen an die IT-Sicherheit gestellt werden. Es ist am Management zu entscheiden, ob in ein aktives Sicherheitsmanagement investiert werden oder ob darauf vertraut werden soll, dass dem Unternehmen das Glück weiterhin treu bleibt und Folgekosten oder Schlimmeres ausbleiben.

Das richtige Mass an Sicherheitsqualität bedingt aktives Management von Risiken, um den Dimensionen Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit gerecht zu werden. Also die gewünschte Qualität in diesen Bereichen zu definieren, mit dem Bewusstsein, dass Qualität auch ihren Preis hat. Es kann nicht das Ziel sein, den ROSI auf Grund von real eintretenden Pannen, die mit einer entsprechenden Investition hätten verhindert werden können, im Nachhinein zu rechtfertigen. Im Fall der IT-Sicherheit geht es um bewusste Investitionsentscheidungen, die vom Topmanagement getroffen werden müssen, um vorbeugend und nachhaltig den erforderlichen Sicherheitslevel zu erreichen. Wesentlich ist, dass die Wirkung der getätigten Investitionen nachgewiesen werden kann. Um das zu erreichen, muss die erreichte Sicherheit messbar sein.

Vier Dimensionen der IT-Sicherheit  
IT-Sicherheit erklärt sich im Wesentlichen anhand von vier Begriffen (oft abgekürzt als CIAN):

- Vertraulichkeit (Confidentiality) kümmert sich darum, dass Informationen entsprechend geschützt werden, um nur nach bestimmten Regeln/Abmachungen den Berechtigten zur Verfügung zu stehen.

- Integrität (Integrity) der Informationen bedeutet, dass diese nicht verändert worden sind (unbeabsichtigt oder böswillig). Informationen müssen also auf ihre Echtheit überprüfbar sein.
- Verfügbarkeit (Availability) von Informationen ist für viele Unternehmen überlebenswichtig.
- Nachvollziehbarkeit (Non-Repudiation) von Informationen ist äusserst wichtig in vielen Bereichen des täglichen Geschäftslebens, zum Beispiel bei einem Vertragsabschluss.

Diese vier Dimensionen können mit Investitions- und Betriebskosten versehen werden. Noch fehlen allerdings die aus dem Kerngeschäft abgeleiteten Anforderungen, Vorgaben und Randbedingungen an die IT-Sicherheit. Es ist nicht definiert, wie man den erreichten Grad an Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit messen kann, um das IST mit dem SOLL zu vergleichen.

Vorgaben, Anforderungen und  
Randbedingungen

Vorgaben sind feste Grössen, die im Unterschied zu Anforderungen nicht verhandelbar sind. Vorgaben kommen von Standesorganisationen, vom Staat, von Organisationen/Vereinen/Fachgruppen oder der eigenen Firma. Beispiele dafür sind der Ethik-Code für Informationssysteme, der Sarbanes-Oxley Act oder der Datenschutz für Patientendaten.

Anforderungen werden von den Stakeholdern in einem geordneten Prozess definiert. Wer sind die Stakeholder im Fall der IT-Sicherheit? Eine Antwort vorweg: Es ist nicht die IT-Abteilung.

Wer hat demzufolge Qualitätsansprüche bezüglich Sicherheit, wenn nicht die IT-Abteilung? Neben dem Topmanagement, das die Ansprüche für die ganze Firma definiert, sind es die Kernprozess-Eigner. Sie sind verantwortlich für die Daten und die Logik für

deren Verarbeitung. Die Rolle der IT beschränkt sich auf die Dienstleistungen (fachliche Beratung, Umsetzung, Betrieb).

Folglich müssen die Kernprozesseigner die Anforderungen an die Sicherheit formulieren – innerhalb der vom Topmanagement definierten Security Policy – mit Bezug auf die vier CIAN-Dimensionen. Die IT soll allerdings in einer partnerschaftlichen Art und Weise mithelfen, diese Anforderungen auf den Boden der Realität zu bringen. Dazu wird ein formelles Anforderungsmanagement benötigt.

Zusätzlich existieren oft Randbedingungen, die klar kommuniziert werden müssen. Die IT-Sicherheitsfachkräfte sind im engen Dialog mit den Verantwortlichen der Geschäftsfelder gefordert, geeignet zu kommunizieren und die heutigen technischen Möglichkeiten real aufzuzeigen. Hier geht es um realistisches Erwartungsmanagement.

#### Preisgestaltung

Der Preis der IT-Sicherheit wird im Wesentlichen durch die Effizienz des Prozesses selbst sowie durch die Einflussgrößen Anforderungen, Vorgaben und Randbedingungen bestimmt. Die Zweiteilung zwischen Business Owner und IT zeigt, dass der Prozess beide Partner braucht und die Effizienz eine Grösse ist, die durch beide Partner beeinflusst wird. Sowohl die Business Owner wie die IT bewegen sich im Umfeld, das vom Topmanagement vorgegeben ist (Security Policy).

Wichtig ist das Bewusstsein, dass die Einflussgrößen durch bewusstes Risikomanagement bis zu einem grossen Grad selbst bestimmbar sind! Dies beginnt mit der durch das Topmanagement vorgegebenen Security Policy, geht über in die Beeinflussung von Randbedingungen, dem Formulieren von vernünftigen Anforderungen und hat nicht zuletzt auch mit der Auswahl der Zusammensetzung der IT-Abteilung oder der Business Owner zu tun. Ebenfalls klar ersichtlich



Kosten der IT-Security: Glücksspiel oder gezielte Investition?

ist die Wichtigkeit des Zusammenspiels aller Beteiligten, um die Effizienz des Prozesses P zu garantieren.

#### Sicherheit messen

Messen heisst vergleichen mit einer Referenzgrösse. Sicherheit kann nicht generell gemessen werden. Es können aber einzelne Bereiche angeschaut und mit einer Referenzgrösse verglichen werden. Nachfolgend ein Beispiel in Bezug auf die Passwortlänge: Ist ein Passwort von fünf Zeichen gut oder schlecht? Wenn die Anforderung definiert, dass ein Passwort minimal acht Zeichen lang sein soll, ist dies sicherlich schlecht. Besteht keine Anforderung, können wir die Beurteilung nicht vornehmen. Gibt es eine Anforderung von minimal vier Zeichen, ist das Passwort gut.

Will man Sicherheit messen, müssen zuerst relevante und als wichtig erachtete Kriterien definiert werden. Es geht auch hier um Anforderungen, Vorgaben und Randbedingungen. Entscheidungen, ob beispielsweise ein Passwort minimal aus vier oder aus acht Zeichen bestehen soll, müssen getroffen werden. Es gilt für jede einzelne Anforderung,

die Risikoabschätzung vorzunehmen und zu entscheiden. Nur wenn der Katalog der Referenzgrößen definiert ist, können diese Werte gemessen werden. Eine Aussage, ob gut oder schlecht bezüglich dieses Kriterienkatalogs, ist dann möglich. In unserem Beispiel mit der Passwortlänge (unter der Annahme, dass wir eine Länge von mindestens acht Zeichen vorgeben), könnte eine Auswertung vorgenommen werden, welche Benutzer ein zu kurzes Passwort haben.

#### Nicht andere entscheiden lassen

Bei der IT-Sicherheit ist es oft so, dass andere für uns entscheiden. Wir verlassen uns auf Erfahrungen Dritter, die eventuell in unserer Umgebung fehl am Platz sind. Firmen verkaufen Lösungen, die angeblich bei der Konkurrenz auch im Einsatz sind. Es wird uns suggeriert, dass wir nur bei einer Höchstverfügbarkeit am Markt bleiben werden. Wir lassen unsere Systeme von unkompetenter Stelle durchleuchten und erhalten einen Testbericht mit vielen dunkelroten Punkten, ohne jeden Bezug zu unserem Kriterienkatalog.

Wo bleibt da das Risikomanagement mit den Anforderungen, Vorgaben und Randbedingungen? Wo bleiben das Messen und die Bewertung gemäss dem Kriterienkatalog?

Nachdem die Zusammenhänge, die zum Preis der IT-Security führen, klar sind, ist auch klar, dass es dafür keine einfache Antwort gibt. Der Preis wird bestimmt durch ein aktives Risikomanagement über alle genannten Dimensionen. Ohne Risikomanagement ist der Preis für die IT-Sicherheit eine nicht voraussehbare Grösse – ein Selbstbedienungsladen ohne Kasse, ein Glücksspiel mit sehr hohem Einsatz und ungewissem Ausgang. ■

