Nr. 2, Mai 2011

<kes>

Die Zeitschrift für Informations-Sicherheit

ISSN 1611-440X

BSI Forum

offizielles Organ des BSI

Bundesamt für Sicherheit in der Informationstechnik

Sonderdruck für

CETUS Training & Consulting

Best Practice für SAP:

Im Dreisprung zu mehr Sicherheit

S. 22

Ausgewogene Sicherheitskosten

durch das richtige SIEM und Controlling

S. 59

SecuMedia

Ausblick auf den **12. Deutschen IT-Sicherheitskongress,** S. 11

Ganzheitliches Sicherheitskosten-Controlling

Regelmäßig müssen Budgets erkämpft und Ausgaben für Informationssicherheit gerechtfertigt werden. Ein Controlling-Modell, das externe Effekte integriert, erleichtert es dabei, betriebswirtschaftliche Vorteile zu berechnen, ohne gegenüber Nachteilen blind zu erscheinen. Die Amortisation von Sicherheitsinvestitionen wird damit solide begründet.

Von Frederik Humpert-Vrielink und Nina Vrielink, Schüttorf

Informationssicherheit ist zu teuer, zu komplex und überhaupt liefern die Einführung von Informationssicherheitsmanagementsystem (ISMS) oder technischen Komponenten keinen messbaren Mehrwert für das Unternehmen – wer kennt solche Aussagen nicht aus dem Munde von Betriebswirten? Doch genau an dem Punkt irren die „Herrscher der Zahlen“: Sicherheit kann nicht nur Kosten produzieren, sondern auch wirtschaftliche Vorteile bedeuten.

Natürlich müssen sich auch Management und Maßnahmen zur Informationssicherheit innerbetrieblich einer genauen Kostenrechnung unterziehen. So einfach sich dies bei manchen technischen Maßnahmen gestaltet, so komplex kann es bei der Einführung strukturierter Managementsysteme werden. Klassische Modelle wie die Betrachtung von Total-Cost-of-Ownership (TCO), Return-on-Investment (ROI), Prozesskosten- oder Vollkostenrechnung stoßen hier schnell an ihre Grenzen, da die belastbare Grundlage für die Berechnung der entsprechenden Kosten- und Nutzenfaktoren fehlt. Beratung und Investitionen in Mitarbeiter sind ja längst nicht alle Effekte, die ein Management-Projekt verursacht – nicht selten treten auch „externe“ Effekte auf.

Besonders deutlich wird dies am Beispiel eines Informationssicherheitsmanagementsystems (ISMS): Die fehlende Berechnungsgrundlage für gängige Modelle liegt geradezu in der Natur eines ISMS. Denn es produziert neben direkten Kosten für Personal und Implementierungsaufwand in erheblichem Maß externe Effekte, die in den genannten Modellen nicht berücksichtigt werden – und zwar entweder, weil die Entwickler der Modelle sie nicht kannten oder bewusst nicht einbeziehen wollen.

Modell aus der Volkswirtschaft

Die Definition eines externen Effektes (auch Externalität) in der Volkswirtschaft ist einfach: Es handelt sich dabei um Auswirkungen ökonomischer Entscheidungen auf Dritte, für die (zumindest zunächst) niemand Zahlungen leistet oder erhält (vgl. http://de.wikipedia.org/wiki/Externer_Effekt). Positive externe Effekte sind beispielsweise Erträge aus einer Erfindung, die nicht dem Erfinder, sondern der umgebenden Gesellschaft zugute kommen (sog. soziale Erträge). Insbesondere liegen solche Effekte vor, wenn ihr Verursacher sie in seinem Kalkül überhaupt nicht berücksichtigt hat – zumeist weil keine Messbarkeit oder Möglichkeiten zur Monetarisierung vorliegen.

Negative externe Effekte entstehen indessen, wenn die Handlung eines Einzelnen die umgebende Gesellschaft so beeinflusst, dass die gesamtgesellschaftliche Wohlfahrt sinkt oder Andere in ihrem Handeln beeinträchtigt werden. Ein Beispiel für derartige „soziale Kosten“ ist die Umweltverschmutzung durch Industrieproduktion.

Volkswirte versuchen, diese Effekte in die Kalkulation der sie verursachenden Wirtschaftssubjekte zu integrieren; diesen Vorgang bezeichnen sie als „Internalisierung externer Effekte“. Bei positiven Effekten geschieht dies über Subventionen, negative externe Effekte werden über Steuern internalisiert, welche die Auswirkungen auf die Gesellschaft ausgleichen (helfen) sollen. Beispiele sind die so genannte „Ökosteuer“ oder die Subvention neuer Entwicklungen in der IT-Sicherheit. Diese Vorgehensweise soll in der Theorie zu einer Balance führen, welche die gesamtgesellschaftliche Wohlfahrt erhöht.

Anwendung auf die Sicherheit

Analog dazu kann der Einbezug der (aus Abteilungssicht) externen Effekte von Sicherheitsmechanismen zum einen die Gesamtbilanz für das Unternehmen verbessern, zum anderen verspricht ein solches Vorgehen sowohl im ganzheitlichen Sinne fundiertere Entscheidungen als auch höhere Akzeptanz von Seiten der Geschäftsführung.

Doch wo liegt nun der Punkt der „optimalen“ Informationssicherheit, der die Gesamtwertschöpfung

des Unternehmens erhöht? Idealerweise fällt dieser Punkt mit der maximalen Sicherheit zusammen, sodass keine Veränderungen vorgenommen werden müssen. Alternativ handelt es sich um den Punkt, an dem Veränderungen im Sicherheitssystem keine Auswirkungen (mehr) auf die Gesamtwertschöpfung haben.

Diesen „idealen Arbeitspunkt" zu ermitteln zählt zu einer der wichtigsten Aufgaben von Beratern, Beauftragten für Informationssicherheit und Controllern. Das ist nicht einfach: Einerseits ist die Ermittlung der externen Effekte nicht trivial – es bedarf eines ausgereiften und strikt durchgeführten Controllings im Unternehmen, um diese Effekte aufzuspüren. Andererseits scheuen viele Organisationen bereits den initialen Aufwand, den der Aufbau ein derartigen Controlling- und Managementsystems bedeutet.

Eine weitere Schwierigkeit folgert aus der notwendigen Betrachtung von Sicherheit *und* Wirtschaftlichkeit: Sollte das Rechenmodell auf ein unwirtschaftliches Sicherheitssystem hindeuten, ist sein Einsatz dennoch im Einzelfall abzuwägen, um nicht komplett von den Zielen der Informationssicherheit abzuweichen und „auf Risiko" zu setzen.

Paradebeispiel ISMS

Doch zurück zum ISMS, das gleich mehrere „Dimensionen" direkter (vor allem Beratungs-, Personal- und Implementierungskosten) und indirekter Kosten besitzt, die beispielhaft in Abbildung 1 dargestellt sind. Negative externe Effekte eines ISMS erstrecken sich oft auf

- Verluste an Produktivität,
- Verringerung der (zumindest kurzfristigen) Wettbewerbsfähigkeit im Vergleich mit Unternehmen, die auf derartige Maßnahmen verzichten oder
- Veränderungen (Verschlechterungen) des Betriebsklimas.

Doch auch positive externe Effekte sind natürlich zu beobachten, etwa

- Auswirkungen der Schadensvermeidung auf Produktion, Produktivität oder Effektivität,
- Verringerung der Kosten potenzieller Schäden,
- ein besserer Schutz vor Wissensabfluss,
- die Einhaltung von Compliance-Regelungen,
- bessere Konditionen bei Kreditverhandlungen,
- Auswirkungen des Managementsystems auf die Wahrnehmung am Markt,

um nur einige Beispiele zu nennen (vgl. Tabelle).

Unter Einbeziehung dieser Indikatoren liegt optimale Sicherheit immer dann vor, wenn die Grenzkosten der Sicherheit den Grenzkosten der Unsicherheit möglichst nahe kommen. Das ist in der Regel dann gegeben, wenn die Kosten der Sicherheit in der gleichen oder geringeren Proportion steigen wie die Kosten der Unsicherheit sinken.

Es sei daran erinnert, dass „optimale Sicherheit" hier nicht „höchste Sicherheitsstandards" bedeutet, sondern genau der Grad an Sicherheit geschaffen wird, der für das betrachtete Unternehmen möglichst viel Informationssicherheit so umsetzt, dass die Geschäftsziele nicht (bzw. möglichst wenig) beeinträchtigt werden. Schließlich soll Informationssicherheit ein Unternehmen ja krisenfester machen und nicht in eine Krise hineinsteuern.

Ohne die Berücksichtigung externer Effekte kann im Extremfall eine drastische „Verteuerung" der Implementierung erst auffallen, wenn es schon zu spät ist – wie im folgenden (stark vereinfachten) „Fall": Nachdem die beispielhafte Blindflug GmbH ein ISMS nach IT-Grundschutz eingeführt hatte, sanken ihre Grenzkosten der Unsicherheit deutlich, da der Grad an IT-Sicherheit erhöht wurde.

Völlig unerwartet stiegen jedoch gleichzeitig die Grenzkosten der Sicherheit überproportional, da eingeführte Sicherheitsmechanismen Auswirkungen auf die Produktion hatten, die im ersten Jahr einen Produktivitätsverlust von 33 % bewirkten, weil Maschinen nicht mehr wie gewohnt funktionierten und häufigere Wartungszyklen mit Ausfallzeiten erforderlich wurden.

Bei 8 % Ertrag und einer Vorjahresproduktionsleistung von 15 Mio. Euro gesellten sich zu den kalkulierten Kosten für organisatorische und technische ISMS-Komponenten von immerhin 400 Tsd. Euro noch Ertragsausfälle von weiteren 400 Tsd. Euro, sodass im Ergebnis die Einrichtung des ISMS (ohne Berücksichtigung weiterer Effekte) doppelt so teuer wurde, wie veranschlagt.

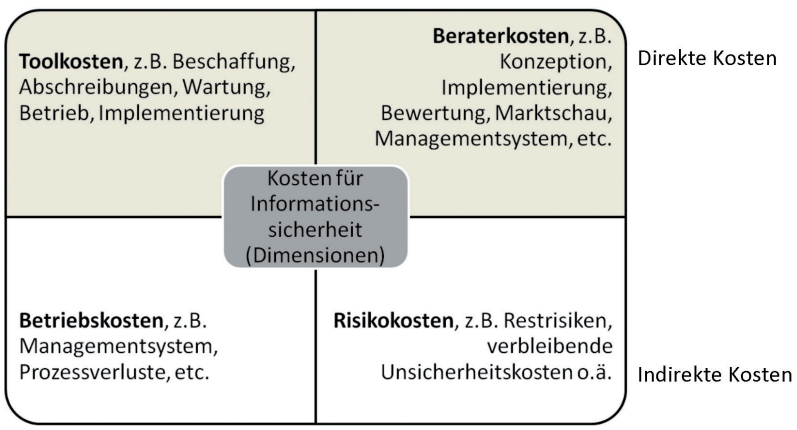

Abbildung 1: Sicherheit bedeutet sowohl direkte als auch indirekte Kosten

Messen und Regeln

Die Messbarkeit externer Effekte verlangt ein reifes Managementsystem, das wiederholbare und wohldefinierte Prozesse umsetzt. Um die externen Effekte vor der Implementierung eines Managementsystems zu schätzen und nach seiner Implementierung zu ermitteln, ist es naturgemäß notwendig, zunächst die Leistungsfähigkeit und die Zielerreichung in Bezug auf die Geschäftsziele vor Einführung eines Managementsystems zu kennen – das wiederum verlangt ein effektives Controlling aller unternehmerischen Disziplinen.

Zur Abschätzung der Auswirkungen selbst ist es sinnvoll, sich vor der Definition von Prozessen Gedanken über

- Implementierungsauswirkungen,
- Effektivität und Effizienz sowie
- Steuerbarkeit

des einzuführenden Managementsystems zu machen.

Die Implementierungsauswirkungen sind abhängig von den ausgewählten Werkzeugen zur Informationssicherheit und deren Integrationstiefe in die Geschäftsprozesse – je nach Tiefe der Integration können diese Auswirkungen positiv oder negativ sein. Zur Verdeutlichung ein Beispiel aus der Praxis: Die fortgeschrittene Integration von Produktionsanlagen in IT-Netze führt zwangsläufig dazu, dass sich Sicherheitsmaßnahmen, die im Gesamtnetz implementiert werden, auch auf diese Anlagen auswirken. Dabei kann es durchaus dazu kommen, dass sie ihren Dienst versagen, weil bestimmte Informationen nicht mehr korrekt übertragen werden können.

Die Effizienz eines eingeführten Managementsystems ist ebenfalls relevant für die Messbarkeit der externen Effekte: So ergeben Kennzahlen der Effizienz in Verbindung mit den Implementierungsauswirkungen aussagekräftige Kontrollzahlen, um die tatsächlichen Auswirkungen einschätzen zu können.

Nicht zuletzt ergeben sich auch durch die Steuerbarkeit des Managementsystems Auswirkungen auf das Controlling-Modell: Je weniger ein Managementsystem steuerbar ist, desto geringer sind die Einflussmöglichkeiten, um negative Auswirkungen an bestimmten Stellen auszuschalten – desto höher sind also beispielsweise die Verluste im Bereich der Produktivität und somit auch die mit dem Einsatz des Managementsystems verbundenen Kosten.

Auf der anderen Seite gibt es jedoch auf Basis der gleichen Kennzahlen auch deutlich messbare

ISMS-Auswirkungen auf	Positive externe Effekte	Negative externe Effekte
Produktion	• Verringerung von Ausfällen der Logistik • Minimierung von Ausfällen wegen Integritätsfehlern	• Verringerung der Produktivität durch Sicherheitsmaßnahmen • Schwierigkeiten, Produktionsanlagen sicher zu gestalten
Verwaltung	• Verhinderung von Wissensabfluss • geringere Schäden durch unsichere IT-Nutzung	• Verschlechterungen des Betriebsklimas • juristische Schwierigkeiten bei Eingriffen in die Arbeitswelt
Externe Parteien (z. B. Kunden/ Lieferanten)	• Erhöhung des Vertrauens in das Unternehmen • potenziell bessere Finanzierungskonditionen	• erhöhtes Ziel für externe Angreifer

Tabelle 1: Beispielhafte externe Effekte von Informationssicherheitsmanagementsystemen (ISMS)

positive Effekte, die den gern als Kostentreiber identifizierten Bereich Informationssicherheit schnell zu einem theoretischen Profit-Center entwickeln können: So ist ein effizientes Managementsystem durchaus in der Lage, eine Imageverbesserung am Markt zu erzielen. Aktuell ist dies gerade im Automobilsektor mit hoher Supply-Chain-Integration zu bemerken, wo die Revisionsabteilungen der Automobilhersteller effiziente Managementsysteme bei ihren Lieferanten abfragen und mit der Macht des Kunden auditieren. Effizient und effektiv arbeitende Managementsysteme können hier einen deutlichen Wettbewerbsvorteil realisieren und damit Kosten senken.

Umsetzung in der Praxis

Den beschriebenen theoretischen Überbau in die Praxis umzusetzen ist ein wichtiger Punkt für den Erfolg der Sicherheitsanstrengungen in Unternehmen: Nur wenn es gelingt, den Controlling-Aspekt so zu gestalten, dass Kosten der Sicherheitsanstrengungen mit ihrem Nutzen in Zusammenhang gebracht werden, ist der Erfolg sichergestellt.

Das ist jedoch längst nicht immer einfach zu erreichen: Welches Unternehmen verfügt schon über ein wohldefiniertes Dokumentationssystem für Sicherheitsvorfälle oder Betriebsstörungen, die man durch optimale Informationssicherheit reduzieren könnte (Nutzenabschätzung)? Und wo unterhält man schon vor Einführung eines ISMS ein eigenes Controlling der Unsicherheitskosten seiner Arbeitsplätze?

Da dies oft nicht der Fall ist, sind viele der hier angestellten Überlegungen beim Projektstart noch Utopie. Hilfreich ist dann die Umsetzung mittels der so genannten Szenariotechnik – hier jedoch in der Form abgewandelt, dass nicht ein Trendszenario mit veränderten Zukunftseinflüssen modelliert wird, sondern das bestehende Szenario konstant bleibt und initiale Modifikationen mit Auswirkungen auf Verfügbarkeit, Vertraulichkeit und Integrität in die Modellierung einbezogen werden. Aus solchen Projektionen lassen sich dann neben den direkten Kosten des Projekts auch die indirekten Kosten je nach Szenario ermitteln. Ein wichtiger Aspekt ist, dabei die unterschiedlichen Szenarien mit Eintrittswahrscheinlichkeiten zu gewichten, um ein verlässliches und aussagekräftiges Bild der tatsächlichen Kosten zu erhalten.

Um dieses Modell letztlich umzusetzen, sind ferner Werkzeuge notwendig, welche die Dokumentation der Zahlen und die Darstellung in Dashboards ermöglichen. Dabei kommen normalerweise speziell auf das Projekt zugeschnittene Formulare zum Einsatz, um die zu messenden Informationen aufzunehmen und auszuwerten – eine Unterstützung mittels webbasierter Dienste ist derzeit am Markt nicht verfügbar.

Bei all dem stellt sich natürlich auch die Frage, wer praktisch für die Umsetzung des Security-Cost-Controlling-Ansatzes zuständig ist: Diese Aufgabe im Controlling des Unternehmens anzusiedeln wäre sicher fatal, da hier zumeist die Meinung „Gut ist, was Geld spart" vorherrscht, wobei der Ansatz, dass billiger immer besser bedeutet, aber generell fehlerhaft und in Sachen Sicherheit zudem noch höchst riskant ist.

Wo das nicht bereits geschehen ist, wird es daher höchste Zeit, dass Sicherheitsmanager ihre angestammte Rolle verlassen und den Betriebswirtschaftlern nur als Mahner und Kostentreiber auffallen. Ein gutes und funktionsfähiges Security-Cost-Controlling zu implementieren setzt voraus, das Thema Sicherheit im Unternehmen auch als Geschäftstreiber platzieren zu können. Dass Finanzinstitute verstärkt Wert auf operationales Risikomanagement legen, gibt diesem Aspekt der Informations-Sicherheitsmanager weiteren Auftrieb.

Als „Türöffner" vor Projektbeginn können beispielsweise die folgenden Fragen dienen, deren Antworten positive externe Effekte versprechen:

_____ Welche Anforderungen haben Banken und Kapitalgeber und welche Verbesserungen treten dort ein?

_____ Welche Anforderungen stellt der Markt und welche Auswirkungen auf das Image stehen bevor?

_____ Wie sind die Lieferketten gestaltet und hat Informationssicherheit hier hohe Priorität?

Fazit

Die Kosten von Informationssicherheit zu ermitteln ist kompliziert und verlangt besonnene Ruhe und Konzentration – spätestens sobald es sich nicht mehr nur um die Investitionen in technische Komponenten handelt. Ein funktional aufgebautes und aussagekräftiges System zum Controlling und zur Messung von Aufwand und Erträgen der Informationssicherheit versetzt Unternehmen jedoch in die Lage, sich ein realistisches Bild zu verschaffen. Dass die dabei errechneten Erträge in Teilen kalkulatorisch sind und Unternehmen keine Liquidität zuführen, dabei nebensächlich. ■

Frederik Humpert-Vrielink ist ISO-27001-Auditor und Handlungsbevollmächtigter, Nina Vrielink ist Geschäftsführerin der CETUS Consulting GmbH.