HMD Praxis der Wirtschaftsinformatik
ISSN 1436-3011
02.06.2006

Kosten & Nutzen von IT-Sicherheit

Einwurf

Was den Nutzen von IT-Sicherheit angeht, bin ich schnell fertig: IT-Sicherheitsfunktionen sind immer dann nützlich gewesen, wenn nichts passiert ist. Das heißt, den Nutzen von IT-Sicherheit kann man weder sehen noch spüren. Darin liegt das Vermittlungsproblem all derer, die sich mit IT- Sicherheit beschäftigen müssen.

Hat man dies erkannt, kann man sich dem Thema Kosten der IT-Sicherheit nun auf zwei Arten nähern: Erstens kann man sachlich argumentieren. So könnte etwa der Sicherheitsbeauftragte eines Unternehmens zu seiner Unternehmensleitung sagen: “Die Produkte unseres Unternehmens sind über die Jahre hinweg mehr und mehr vom zuverlässigen Funktionieren der IT abhängig geworden. Dadurch wachsen die Anforderungen an die Sicherheit unserer Systeme. Ich brauche mehr Geld zur Absicherung unserer Systeme.“ Antwort des Geschäftsführers: “Geld haben wir dafür leider keines.“ Weiter in Gedanken: “Du kommst uns schon teuer genug!“ Dann sagt er: “Aber wenn Sie schon mal hier sind: Könnten wir nicht hier oben auf der Vorstandsetage so ein Wireless LAN einrichten? Mein Sohn hat sowas jetzt bei uns zu Hause, mit WEP und so. Das ist doch sicher, oder? Da komme ich ganz bequem mit meinem Laptop ins Internet. Das möchte ich auch hier so haben!“

Hier die Alternative: Der Sicherheitsbeauftragte präsentiert der Geschäftsleitung eine Kurve, die stark nach oben zeigt. (Der Geschäftsführer freut sich schon, weil er denkt, es sind die Umsätze.) “Hier eine Statistik, wie vielen Angriffen wir täglich ausgesetzt sind.“ Was er nicht sagt: Die Statistik zeigt die gestiegene Anzahl von eingehenden Datenpaketen, die an der Firewall des Unternehmens abgewiesen werden. Derartige Statistiken sind für beide Seiten nützlich: Der Sicherheitsbeauftragte kann zeigen, dass weiteres Geld locker gemacht werden muss, weil es sonst ganz schlimm kommt. Das treibt natürlich die Kosten der IT-Sicherheit weiter in die Höhe, beruhigt aber wiederum die Geschäftsleitung. Nebenbei sieht der Sicherheitsbeauftragte, dass die bisher ergriffenen Maßnahmen wirken, was er natürlich für sich behält. Eine in 2004 von WatchGuard durchgeführte Befragung von 150 IT- (Sicherheits-)Experten ergab, dass knapp die Hälfte (49%) aller Befragten diese Methode verfechten und 29% sogar mit Einschüchterungen arbeiten, um ihre Geschäftsführung zu “überzeugen“. Die beschriebene Form der Angst- und Verunsicherungsmethode (engl. Fear, Uncertainty and Doubt, kurz: FUD) ist also offenbar weit verbreitet.

Seriöses Sicherheitsmanagement verfolgt momentan hauptsächlich qualitative und nur sehr eingeschränkt auch quantitative Ansätze. Die qualitativen Ansätze, beispielsweise der internationale Standard ISO 17799 oder das deutsche Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik, haben gemeinsam, dass sie “Best Practices“ formulieren, die mehr oder weniger auf die eigene Organisation passen. Das Hauptproblem solcher Best Practices ist der Mainstream- Ansatz. Wenn alle das Gleiche machen, machen sie auch die gleichen Fehler; dies gilt natürlich auch im Sicherheitsbereich. Seit einigen Jahren lasse ich die Studenten zu Beginn der Übungen zu meinen Vorlesungen “IT- Sicherheit“ und “Sicherheitsmanagement“ über die seit der letzten Übung bekannt gewordenen Sicherheitslücken und Probleme berichten. Es ist eindrucksvoll, mit welcher Regelmäßigkeit immer wieder die gleichen Lücken auftreten: Unsichere Browser, Würmer, Trojanische Pferde, Identitätsklau – und wieder Angst und Verunsicherung. Schon deshalb lohnt es sich manchmal, gegen den Strom zu schwimmen. Heterogenität, Diversität und die Nutzung verteilter Systeme waren und sind zur Verbesserung der Sicherheit selten schädlich!

Damit komme ich zum schwierigeren Teil. Ein quantitativer Ansatz sollte das Messbare messen und das Zählbare zählen. Am Beispiel des Risikos als Produkt aus Eintrittswahrscheinlichkeit eines Ereignisses (zählbar) und dessen Schaden (messbar) wird die Problematik deutlich: Quantitative Ansätze setzen empirische Daten voraus, die möglichst über viele Unternehmen hinweg akkumuliert werden sollten. Bei den Ereignissen (Sicherheitsvorfälle, Angriffshäufigkeit) gelingt dies inzwischen recht gut. Jedes halbwegs gute Intrusion- Detection-System besitzt eine Reporting-Funktion. Auch das Akkumulieren gelingt schon einigermaßen, denn Sicherheitsdienstleister erfassen und klassifizieren die bei ihren Kunden aufgetretenen Vorfälle, und die Foren und Mailinglisten der Computer Emergency Response Teams (CERTs) erlauben auch Rückschlüsse auf die Quantität von Vorfällen im Großen. An der Erfassung der durch diese Ereignisse entstandenen Schäden hapert es dagegen bisher. Niemand lässt sich gern in die Karten schauen, wenn es ums Geld geht. Zu groß wäre der Imageverlust, wenn bekannt würde, welche Schäden ein Unternehmen durch Computerbetrug, Viren, bösartige Mitarbeiter etc. erlitten hat.

Da aber Sicherheitsmaßnahmen üblicherweise ergriffen werden, um Schäden in der Zukunft abzuwehren, sollten möglichst viele Datenquellen nutzbar sein. Eine Forschungsfrage der Zukunft ist, ob und wie die Erhebung von Schäden unter Wahrung des Betriebs- und Geschäftsgeheimnisses möglich ist. Anschließend stellt sich die Frage, wie ein einheitliches Vorgehen aussieht und welche Metriken die Vergleichbarkeit der Daten ermöglichen. Schließlich ist die Frage zu beantworten, wie quantitatives IT-Sicherheitsmanagement in den Gesamtablauf des Controllings integriert werden kann. Da IT-Sicherheit ein Querschnittsthema ist, existieren starke Wechselwirkungen mit den anderen Abläufen eines Unternehmens, eine Kosten-Nutzen-Optimierung von IT- Sicherheit erfordert also stets eine betriebswirtschaftliche Gesamtbetrachtung.

Sicherheit ist – wie zu Beginn erwähnt – gerade dann vorhanden, wenn nichts passiert – oder wenn sich bisher niemand für das “Schutzgut“ interessiert hat. Man sollte es also auch mal positiv sehen: Massiven Angriffen ausgesetzt zu sein, kann auch als Indikator für Sichtbarkeit und Erfolg im Markt bewertet werden. Und plötzlich wird IT-Sicherheitsmanagement zum kostengünstigen Controlling-Instrument eines Unternehmens.

Prof. Dr. Hannes Federrath
Universität Regensburg
Lehrstuhl Management der Informationssicherheit
Universitätsstr. 31
93053 Regensburg
hannes.federrath@wiwi.uni-regensburg.de
www-sec.uni-regensburg.de

HMD, Heft 248, April 2006