


Bezahlbare Informatik-Sicherheit durch Zusammenarbeit

von Alexander Colombi und
Kurt Rechsteiner



Mit der Ausbreitung der Informatik haben auch die damit verbundenen Bedrohungen und Schäden massiv zugenommen. Dabei wird oft übersehen, dass die Gefahren weniger von der Technik als vom Faktor Mensch und von organisatorischen Mängeln ausgehen. Wie können Unternehmen eine adäquate IT-Sicherheitskultur aufbauen? Wie können sie die Wahrscheinlichkeit und die Tragweite von Schäden auf ein tolerierbares Restrisiko eingrenzen, ohne dafür unzumutbar viele Ressourcen einzusetzen?

Das Schadenspotenzial von IT-Störungen ist enorm, und es nimmt weiter zu. Nun wäre das nicht weiter schlimm, wenn es denn beim Potenzial bliebe. Das tut es aber nicht: Auch die real verursachten Schäden erreichen schwindelerregende Beträge. So kam etwa KPMG in ihrer weltweiten Studie „Global Information Security Survey 2002“ auf direkte Verluste von 160.000 Schweizer Franken pro Schadenereignis. Und nach den jährlichen Erhebungen von FBI und Computer Security Institute melden zwei Drittel der Unternehmen Sicherheitsvorfälle.

Ursachen: Mensch und Maschine

Verfügbarkeit, Vertraulichkeit und Integrität müssen gewährleistet sein. Gefährdet werden sie sowohl durch technische Störungen als auch durch organisatorische Unzulänglichkeiten. Dabei ist der Blick allzu oft auf die Technik gerichtet: Das Netzwerk fällt aus, eine Festplatte crasht, die Serverfarm steht unter Wasser, die Datenbank ist korrupt. Übersehen wird dabei der „Faktor Mensch“ beziehungsweise die Organisation: Nach einer Untersuchung des britischen Department of Trade and Industry geht ein Drittel bis zur Hälfte aller Si-

cherheitsvorfälle auf das Konto der eigenen Mitarbeiter.

Der technischen Sicht folgend sind auch Sicherheitsprüfungen oft technisch orientiert. Seltener beziehen sie die organisatorische/menschliche Seite angemessen mit ein. Dabei wäre dies auf verschiedensten Wegen möglich, beispielsweise mit Ethical Hacking durch Tiger Teams (Fachleute, die versuchen, die eigenen Informations- und Kommunikationssysteme anzugreifen, um dadurch Schwachstellen herauszufinden), fingierten Server- und PC-Diebstählen, Tests nach IT-Schulungen und Mitarbeiter-einführungen oder periodischen Befragungen und Audits.

Natürlich sind Art und Umfang der Prüfungen abhängig von der gelebten Sicherheitskultur: Die Einhaltung von Security Policies beispielsweise kann nur geprüft werden, wenn diese auch formuliert und die Mitarbeitenden dafür sensibilisiert sind.

Sicherheitsaudits

Ein periodischer IT-Sicherheitsaudit hilft als präventive Massnahme, mögliche Fehler zu verhindern und das Sicherheitsbewusstsein bei allen Beteiligten in den Bereichen bauliche Sicherheit, Hard- und Software, Daten, Kommunikation und Organisation zu fördern.

Der Audit baut auf Bestehendem auf und ist Teil der Standard-Sicherheitsorganisation des Unternehmens. Wenn die aus dem Audit resultierenden Empfehlungen für Verbesserungsmassnahmen umgesetzt werden, entlastet das die letztlich verantwortlichen Führungsgremien wirksam (zum Beispiel Verwaltungsrat und Geschäftsleitung).

Aufwand reduzieren

Der Aufwand für eine seriöse Sicherheitsprüfung ist hoch und fällt vor allem immer wieder an. Wie kann er auf ein tragbares Mass reduziert werden?

Sparpotenzial 1: Kooperation

Kooperationen sind heute in verschiedensten Ausprägungen, auch unter direkten Konkurrenten, durchaus gängig. Bekannt sind etwa Branchenverbände, Einkaufsge-

meinschaften, Erfa-Gruppen und „best practice“-Verbünde. Sie bieten vielfältige Vorteile, von der Synergienutzung durch Arbeitsteilung bis zur Erweiterung des Blickfeldes (Blick von Aussen, Vermeiden von Betriebsblindheit, „Lernen vom Besten“, bessere Einkaufskonditionen, usw.). Allerdings kämpfen Kooperationen auch mit potenziellen Schwächen: Sie funktionieren nur, wenn die Mitwirkenden bereit sind, sich vertrauensvoll zu öffnen. Und sie neigen gelegentlich zu Schwerfälligkeit, wenn sie nicht bewusst schlank gehalten werden.

Sparpotenzial 2: Standardisierung

Make or buy – stellt sich die Frage überhaupt noch? Nein: Das Rad ist erfunden. Aber nicht jedes Rad passt zu jedem Fahrzeug. Checklisten, Pläne und Erfahrungen sind an die Besonderheiten der Institution anzupassen (Masskonfektion). Doch mit der Standardisierung können enorme Finanzmittel eingespart werden.

Sparpotenzial 3: Externe Spezialisten

Self Assessments scheinen verlockend, weil sie nichts kosten (was natürlich nicht stimmt), sind aber gefährlich: Eine unkritische Selbstüberprüfung mit veralteten „eingerosteten“ Prüflisten verdeckt mehr, als sie Lücken und Schwachstellen aufzeigt.

Externe Spezialistenkenntnisse und Erfahrungen bringen da mehr, bei einer Sicherheitsprüfung so gut wie bei unserem periodischen Gesundheits-Check, für den wir ja auch zum Arzt gehen. Vor allem bei der Diskussion der Massnahmen können sie Erfahrungen und neueste Technologieansätze mit einbringen.

Besonderheiten übergreifender Audits

Bei unternehmensübergreifenden Audits sind einige Aspekte speziell zu beachten: Die Organisation ist, abgestimmt auf die Kooperationsteilnehmer, zu planen. Wie weit geht die Masskonfektion, wo werden also Besonderheiten der Teilnehmergruppe berücksichtigt? Wo findet der Pilot-Audit statt? In welchem Rhythmus folgen die anderen?



Alexander Colombi, lic.oec.inform.
HSG, Vorsitzender der Geschäftsleitung der CSP AG

Seit über zehn Jahren in verschiedenen leitenden Funktionen im Gesundheitswesen tätig. Spezialgebiete: KIS, Verwaltungslösungen, Spitalkooperationen, Strategie- und Organisationsentwicklung



Kurt Rechsteiner, lic.oec.publ.,
Projektleiter der CSP AG

Seit 1964 in verschiedensten Arbeitsgebieten der Informatik und Betriebswirtschaft tätig. Schwerpunkt der letzten 19 Jahre: Informatik im Gesundheitswesen (Strategie, Projekte, Betrieb).

Kooperation ist auch bei den Verbesserungsmassnahmen angesagt, doch es werden voraussichtlich gemeinsam wie auch individuell umzusetzende Massnahmen empfohlen. Da muss differenziert werden. Und schliesslich: Verantwortung kann nicht delegiert werden. Letztlich ist jede Unternehmensleitung für die Sicherheit ihres Geschäftes verantwortlich.

www.csp-ag.ch