Kooperieren in der IT-Sicherheit

Gemeinsam wirtschaftlich sicher

Mit unternehmensübergreifenden Kooperationen können KMU eine adäquate IT-Sicherheitskultur aufbauen. Heisst: Die Wahrscheinlichkeit und die Tragweite von Schäden lassen sich auf ein tolerierbares Restrisiko eingrenzen, ohne dafür unzumutbar viele Ressourcen einzusetzen.

■ Von Alexander Colombi und Kurt Rechsteiner

Das Schadenspotenzial von IT-Störungen ist enorm, und es wächst aus vielfältigen Gründen weiter: zunehmende Vernetzung, fehlerhafte Software, wachsende Datenbestände, überforderte Benutzer usw.

Nun wäre dies nicht weiter schlimm, wenn es beim Potenzial bliebe. Dies tut es aber nicht:

■ Auch die real verursachten Schäden erreichen schwindelerregende Beträge. So kam etwa KPMG [1] in einer weltweiten Studie auf direkte Verluste von CHF 160 000 pro Schadenereignis. Und nach den jährlichen Erhebungen von FBI und Computer Security Institute melden zwei Drittel der Unternehmen Sicherheitsvorfälle.

Mensch und Maschine als Ursachen

Verfügbarkeit, Vertraulichkeit und Integrität müssen gewährleistet sein. Gefährdet werden sie sowohl durch technische Störungen als auch durch organisatorische Unzulänglichkeiten. Bei Kontrollen ist der Blick allerdings (allzu) oft auf die Technik gerichtet: Das Netzwerk fällt aus, eine Disk crasht, die Serverfarm steht unter Wasser, die Datenbank ist korrupt. Übersehen wird dabei der «Faktor Mensch» bzw. die Organisation.

■ Nach einer Untersuchung des britischen Department of Trade and Industry gehen zur Hälfte aller Sicherheitsvorfälle auf das Konto der eigenen Mitarbeitenden: Eine zentrale Netzwerkkomponente ist irrtümlich nicht an die USV angeschlossen, Systeme werden nicht proaktiv überwacht, die Datenbank wird «auf Zuruf», das heisst ohne seriöse Vorbereitung, erweitert.

Nicht nur Technik prüfen

Informatiker sind meist eher technisch orientierte Spezialisten. Deshalb sind auch IT-Sicherheitsprüfungen oft techniklastig. Back-up, Virenscanner und Firewall dürfen sicher nicht vernachlässigt werden. Aber seltener werden organisatorische und menschliche Aspekte angemessen miteinbezogen. Dabei wäre dies auf verschiedensten Wegen möglich, beispielsweise:

■ Mit beauftragten Einbruchsversuchen (Ethical Hacking) und fingierten Diebstählen (Tiger Teams).
■ Mit Usability Checks (endbenutzerunterstützte Funktions- und Tauglichkeitsprüfung).
■ Mit Kurztests nach IT-Schulungen und Mitarbeitereinführungen.
■ Mit periodischen Befragungen und Audits.

Selbstverständlich sind Art und Umfang der Prüfungen abhängig von der gelebten Sicherheitskultur: Die Einhaltung von Security Policies beispielsweise kann nur geprüft werden, wenn Policies auch formuliert und die Mitarbeitenden dafür sensibilisiert sind. Dies gilt sowohl für den laufenden Betrieb als auch für die selbstverständlichen Sicherheitselemente in Projekten.

Zentrales Instrument: Der Audit

Empfehlenswert ist ein periodischer IT-Sicherheitsaudit, denn er hilft präventiv, Überflüssiges wie auch kritische Lücken zu erkennen.

■ Dabei ist nicht nur die Informatik, sondern auch der Endbenutzer mit einzubeziehen. Dadurch wird bereits während der Analyse das Sicherheitsbewusstsein bei allen Beteiligten bezüglich baulicher Sicherheit, Hard- und Software, Daten, Kommunikation und Organisation gefördert.

Der Audit ist Teil der Standard-Sicherheitsorganisation des Unternehmens. Wichtig ist, aus dem Audit mögliche Massnahmen zu priorisieren und zu realisieren.

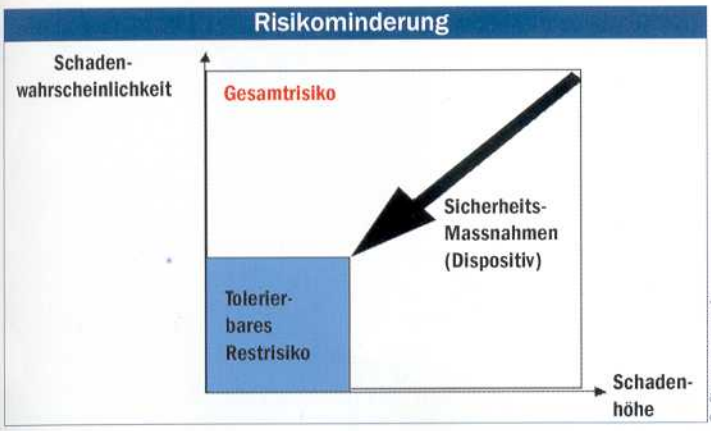
■ Dabei gilt: Weniger ist mehr, wenn das Wenige konsequent umgesetzt wird.
■ Durch die aus dem Audit resultierenden Verbesserungen wird letztlich das verantwortliche Führungsgremium wirksam entlastet (z.B. Verwaltungsrat und Geschäftsleitung).

Allerdings: Der Aufwand für eine seriöse Sicherheitsprüfung ist hoch und fällt vor allem immer wieder an, weil laufend neue Technologien und Bedrohungen zu berücksichtigen sind. Auch die Umsetzung von Massnahmen kostet mindestens personelle, meist auch finanzielle Mittel. So berechnen etwa Banken die Kosten für die IT-Sicherheit mit 15 Prozent der IT-Infrastrukturkosten, 10 Prozent der IT-Betriebskosten und mit 3 bis 5 Prozent des IT-Personals [2].

Sparpotenziale nutzen

Die meisten KMU können sich einen derart hohen Mitteleinsatz nicht leisten. Wie lässt er sich auf

Kooperation von Unternehmen: Auch empfehlenswert im Bereich IT-Sicherheit, um Sicherheitsmassnahmen gemeinsam und damit kostengünstig(er) umzusetzen.



Absolute IT-Sicherheit gibt es nicht: Ziel ist deshalb, das Risiko auf ein tolerierbares Mass zu senken.

ein tragbares Mass reduzieren? Aus unserer Projekterfahrung haben sich vier konkrete Sparpotenziale herausgestellt:

1. Unternehmensübergreifende Sicherheitskooperationen.
2. Nutzung von Sicherheitsstandards.
3. Gemeinsame Audits.
4. Gezielter Einsatz von externen Spezialisten.

1 Sicherheits-Kooperationen

Kooperationen sind heute auch unter direkten Konkurrenten durchaus gängig. Bekannt sind etwa Branchenverbände, Einkaufsgemeinschaften, Erfa-Gruppen und «best practice»-Verbunde. Auch für die IT-Sicherheit können Kooperationen aufgebaut werden.

- Kooperationen bieten viele Vorteile, von der Arbeitsteilung über die Erweiterung des Blickfelds bis hin zur kostengünstigen Umsetzung von Sicherheitsmassnahmen.
- Der Erfolg der Kooperation liegt im Erkennen und bewussten Nutzen dieser Vorteile.

Allerdings kämpfen Kooperationen auch mit potenziellen Schwächen: Sie funktionieren nur, wenn die Mitwirkenden bereit sind, sich vertrauensvoll zu öffnen. Und sie neigen zu Schwerfälligkeit, wenn sie nicht bewusst schlank gehalten werden.

2 Nutzung von Standards

Um nicht das Rad neu erfinden zu müssen, wird immer mehr an (de facto-)Standards, beispielsweise an ISO oder ITIL, angelehnt. Diese helfen, die Prozesse zu optimieren. Sie sind aber stets nur Skelette, die für das jeweilige Unternehmen mit Fleisch zu füllen sind. In der Summe können über die Jahre mittels Standardisierung enorme Finanzmittel eingespart werden.

3 Gemeinsame, übergreifende Audits

Unternehmensübergreifende Kooperationen entwickeln oft spezifische Audits, in die branchen- oder gruppenspezifische Besonderheiten eingebracht werden.

- Die Durchführung der Audits ist abgestimmt auf die Kooperationsteilnehmer zu planen. Wie weit geht die Masskonfektion? Wo werden Besonderheiten einzelner berücksichtigt? Wo wirken Externe, wo Teilnehmer aus der Gruppe als Auditoren? Wo findet der Pilot-Audit statt? In welchem Rhythmus folgen die anderen?
- Kooperation ist auch bei den Massnahmen angesagt, aber: Es werden voraussichtlich sowohl gemeinsame wie auch individuell umzusetzende Massnahmen empfohlen. Da muss differenziert werden.

Der Aufwand reduziert sich durch Kosten- und Erfahrungsteilung. Und auch der Umsetzungserfolg wird mit den Partnern vergleichbar.

4 Externe Spezialisten

Selbstbeurteilungen verlocken auch bei Audits, weil sie nichts zu kosten scheinen (was selbstverständlich nicht stimmt). Sie sind aber gefährlich: Eine unkritische Selbstüberprüfung mit veralteten, «eingerosteten» Prüflisten verdeckt mehr, als sie Lücken und Schwachstellen aufzeigt. Und Selbstkritik ist eine schwierige Disziplin ...

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

Fazit: Gemeinsam wirtschaftlich sicher

Technische und organisatorische Informatik-Sicherheit ist ein an Bedeutung wachsendes, unumgängliches Thema. Auch KMU müssen diese Aufgabe wahrnehmen, für welche letztlich die Unternehmensleitung verantwortlich ist. Die Frage lautet nicht «Sollen wir, oder sollen wir nicht?», sondern vielmehr «Wie können wir den geforderten Sicherheitsstand wirtschaftlich erreichen?».

Dazu drängen sich Kooperationen auf, welche die Sicherheit kostenteilig anhand von Standards optimieren. Basierend auf gemeinsamen, punktuell durch externe Spezialisten unterstützten Audits können die vernünftigen Massnahmen realisiert werden. Motto: Gemeinsam wirtschaftlich sicher.

QUELLEN
[1] KPMG, Global Information Security Survey 2002.
[2] H. Lubich, Referat an der IT-Security-Konferenz, 9. April 2003.

AUTOREN
Alexander Colombi, lic.oec. inform. HSG, ist Vorsitzender der Geschäftsleitung der CSP AG, St.Gallen und Bern. Er ist seit über zehn Jahren in leitenden Funktionen in Informatik und Gesundheitswesen tätig. Er lebt mit seiner Familie in Mörschwil und erholt sich beim Süss- und Salzwasser-Segeln.

Tel. 071 221 10 61
Fax 071 221 10 70
alexander.colombi@csp-ag.ch

Kurt Rechsteiner, lic. oec. publ., ist seit 1964 in verschiedensten Arbeitsgebieten der Informatik und Betriebswirtschaft aktiv, seit 2000 als Projektleiter bei der CSP AG, St.Gallen und Bern. Einen Ausgleich zur Informatik hat er in einem Goggo-Roller, Jahrgang 1953, gefunden.

Tel. 071 221 10 65
Fax 071 221 10 70
kurt.rechsteiner@csp-ag.ch

Die CSP AG, St.Gallen und Bern, ist auf die unabhängige, professionelle Leitung von komplexen Informatik- und Organisationsprojekten spezialisiert. Dazu stehen erfahrene und motivierte Mitarbeiter/-innen im Einsatz, die mit qualitätsgesicherten Projektmethoden arbeiten. Die CSP AG ist in einer flachen Struktur mit Competence Teams organisiert. Branchenschwerpunkte sind Gesundheitswesen, Finanzinstitute, Öffentliche Verwaltungen sowie KMU.

ONLINE
www.csp-ag.ch