Roger Hangartner
Geschäftsführer,
Hangartner & Partner AG,
Freienbach
www.hangartner-partner.ch

Thomas Scheibmayr
Senior Security Consultant,
Hangartner & Partner AG,
Freienbach
www.hangartner-partner.ch

IT-Sicherheit im Unternehmen ist Chefsache!

Treuhandunternehmen verwalten nicht nur die Finanzen ihrer Kunden, sondern zwangsläufig auch die sensitiven Daten der Kundschaft.

Dabei sind sich die Geschäftsführer oftmals gar nicht bewusst, welche Unternehmensrisiken bei der Verarbeitung und Speicherung von Kundendaten eingegangen werden. Die versehentliche Weitergabe, der Verlust oder der Diebstahl von Kundeninformationen kann einen Vertrauensverlust nach sich ziehen, der das Unternehmen gefährden kann. Finanzielle Forderungen über den zivilrechtlichen Weg beschleunigen zudem den drohenden Untergang. IT-Sicherheit ist in Treuhandunternehmen wie auch in anderen KMU oft kein Thema. Meist wird dem PC-Installateur vertraut, dass der schon alles richtig «eingestellt» hat. Die Verantwortung für das Unternehmen trägt aber nicht der IT-Fachmann, sondern vielmehr gilt: Sicherheit ist Chefsache!
Eine weit verbreitete Fehleinschätzung betrifft den eigenen Schutzbedarf. Oft stösst man auf die folgenden Aussagen:

«Bei uns ist noch nie etwas passiert.»
Diese Aussage ist mutig. Vielleicht hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt!

«Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht.»
Diese Einschätzung ist in den meisten Fällen zu oberflächlich. Bei sorgfältiger Betrachtung von möglichen Schadensszenarien zeigt sich schnell, dass durchaus Daten verarbeitet werden, die vielfältigen Missbrauch ermöglichen, wenn sie in die falschen Hände fallen. Ausserdem wird in der Regel nicht beachtet, dass Kunden- und auch Mitarbeiterdaten höchst sensitiv und damit überaus schützenswert sind!

«Unser Netz ist sicher.»
Die Fähigkeiten potenzieller Angreifer werden oftmals unterschätzt. Hinzu kommt, dass selbst erfahrene Netzwerk- oder Sicherheitsspezialisten nicht alles wissen und gelegentlich Fehler machen. Externe Überprüfungen decken nahezu immer ernste Schwachstellen auf und sind ein guter Schutz vor «Betriebsblindheit».

«Unsere Mitarbeiter sind vertrauenswürdig.»
Verschiedene Statistiken zeichnen leider ein anderes Bild: Die Mehrzahl der Sicherheitsverstösse wird durch eigene oder externe Mitarbeiter verursacht. Dabei muss nicht immer Vorsatz im Spiel sein. Auch durch Versehen, Übereifer oder Neugierde gepaart mit mangelndem Problembewusstsein entstehen manchmal grosse Schäden.
Sie sollten sich bewusst machen, dass Sicherheit kein statischer Zustand ist, sondern ein ständiger Prozess, welcher durch den ständigen Wandel von neuen Technologien oder geänderten Anforderungen angetrieben wird. Stellen Sie sich daher immer wieder die folgenden Fragen:

- Was für Auswirkungen hat das für ihr Unternehmen, wenn ein Mitarbeiter mit ihrem Kundenstamm zur Konkurrenz wechselt?
- Welche Konsequenzen hat es für Sie, wenn wichtige Informationen über Finanztransaktionen ihrer Kundschaft plötzlich in der Presse erscheinen?
- Was würde geschehen, wenn in Ihrer Organisation wichtige Computer oder andere IT-Komponenten plötzlich ausfallen und über einen längeren Zeitraum (Tage, Wochen usw.) nicht mehr nutzbar wären? Könnte die Arbeit fortgesetzt werden? Wie hoch wäre der mögliche Schaden?
- Was würde es für Sie heissen, wenn sich beim Jahresabschluss herausstellt, dass viele Daten vom Buchhaltungssystem falsch verarbeitet bzw. nachträglich verändert wurden?

Eine weit verbreitete Ansicht ist, dass IT-Sicherheitsmassnahmen zwangsläufig mit hohen Investitionen in Sicherheitstechnik und der Beschäftigung von hoch qualifiziertem Personal verknüpft sind. Dem ist jedoch nicht so. Die wichtigsten Erfolgsfaktoren sind jedoch gesunder Menschenverstand, durchdachte organisatorische Regelungen sowie zuverlässige und gut informierte Mitarbeiter, die selbstständig Sicherheitserfordernisse diszipliniert und routiniert beachten. Die Erstellung und Umsetzung eines wirksamen und effektiven IT-Sicherheitskonzeptes muss darum nicht zwangsläufig unbezahlbar sein. Die wirksamsten Massnahmen sind überraschend simpel und noch dazu oft kostenlos!

Die meisten Versäumnisse

Bei einer Analyse der typischen Fehler und Versäumnisse finden sich nur geringe Abhängigkeiten zu Unternehmensgrösse und Branche. Anhand der folgenden Liste können Sie leicht überprüfen, welche spezifischen Versäumnisse in Ihrem Umfeld eine Rolle spielen und wie dieser Sachverhalt zu bewerten ist.

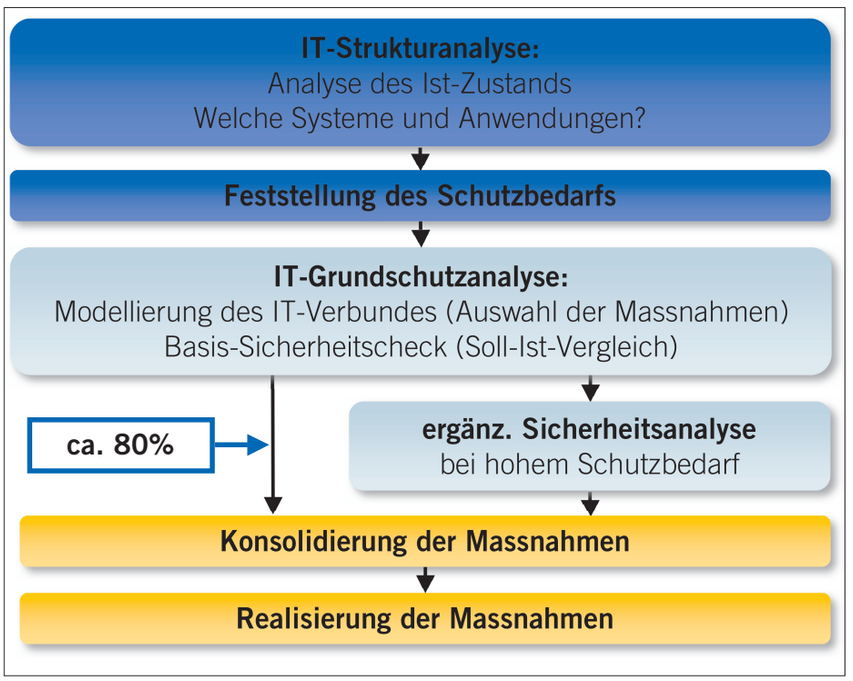
Sicherheit hat einen zu geringen Stellenwert

IT-Sicherheit hat im Vergleich mit anderen Anforderungen (Kosten, Bequemlichkeit, grosse Funktionalität usw.) häufig einen zu geringen Stellenwert. Stattdessen wird IT-Sicherheit als Kostentreiber und Behinderung gesehen. Besonders bei Neuanschaffungen werden Sicherheitseigenschaften einer Anwendung oder eines Systems häufig vernachlässigt oder gar nicht bedacht. Ein Beispiel in diesem Zusammenhang ist die rasant wachsende Zahl völlig ungesicherter drahtloser Netzwerke, seit entsprechende WLAN-Karten preiswert für jedermann zur Verfügung stehen. Begeisterung für eine neue Technik und die Möglichkeit, auf lästige Verkabelung verzichten zu können, lassen Sicherheitsaspekte vergessen. Unzählige Firmen «veröffentlichen» somit unfreiwillig ihre vertraulichen Daten und bieten teilweise allen Interessierten kostenlose Internetzugänge an

Sicherheitsmassnahmen werden aus Bequemlichkeit vernachlässigt

Die besten Sicherheitsrichtlinien und -funktionen helfen nichts, wenn sie nicht beachtet oder nicht genutzt werden. Vertrauliche Dokumente oder E-Mails werden oftmals nicht verschlüsselt, selbst wenn geeignete Mechanismen zur Verfügung stehen. Sichere, regelmässig geänderte Kennwörter werden ebenso als lästig empfunden wie Bildschirmschoner mit Kennwort. Einem x-beliebigen Anrufer, der sich als neuer Mitarbeiter der IT-Abteilung ausgibt, werden Passwörter verraten, wenn er nur «nett» danach fragt.

Daten, insbesondere von Notebooks, werden selten oder sogar nie gesichert, obgleich den Beteiligten die hohen Risiken eines Datenverlustes durchaus bekannt sind. Selbst wenn regelmässige Datensicherungen durchgeführt werden, sind diese oft unvollständig oder fehlerhaft. Mit einer stichprobenartigen Überprüfung der Datensicherung könnte dieses grosse Risiko ausgeschaltet werden! Bei automatisierten Sicherungen wissen Mitarbeiter oftmals gar nicht, welche Daten in welchen Abständen gesichert werden und wie lang die Sicherungsmedien aufbewahrt werden. Zahlreiche weitere Beispiele ähnlicher Art existieren und belegen,



Der standardisierte Ablauf des Sicherheitsaudits ermöglicht ein strukturiertes und zeitsparendes Vorgehen.

dass selbst einfache Sicherheitsmassnahmen zum Scheitern verurteilt sind, wenn deren Durchführung keine Akzeptanz findet oder sie nicht technisch erzwungen werden. Dies gilt leider nicht nur für Anwender, sondern auch für Administratoren.

Verfügbare Sicherheits-Updates werden nicht eingespielt

Viele durch Viren oder Würmer entstandene Schäden treten erst geraume Zeit nach dem ersten Bekanntwerden des Schädlings auf. Zu diesem Zeitpunkt gibt es in der Regel bereits Sicherheitspatches von den jeweiligen Herstellern. Inzwischen werden zu den meisten Produkten Sicherheitspatches in sehr kurzen Abständen veröffentlicht. Auswahl und Tests der im eigenen Kontext tatsächlich relevanten Patches beanspruchen zusätzliche Zeit. Viele Administratoren warten daher lieber bis zur Installation des nächsten regulären Software-Updates und spielen Sicherheitspatches damit nicht rechtzeitig ein. Ein solches Verhalten ist nicht nachlässig, sondern eher (grob-)fahrlässig.

Sorgloser Umgang mit Passwörtern und Zugangsinformationen

Nach wie vor werden die meisten Zugangsschutzverfahren auf Basis von Passwortabfragen realisiert. Dies führt immer dann zu Problemen, wenn unsichere (z. B. zu kurze oder leicht erratbare) Kennwörter gewählt werden. Tagtäglich finden Einbrüche in IT-Systeme statt, weil ein Angreifer erfolgreich – wahlweise durch systematisches Ausprobieren, Raten oder Ausspähen – ein Passwort «geknackt» hat. Das sprichwörtliche Aufbewahren von Passwörtern unter der Tastatur oder in der obersten Schreibtischschublade macht es Tätern mit Zugang zu den Büroräumen besonders leicht, an sensitive Informationen heranzukommen!

Ungenügender Schutz gegen Diebstahl oder Elementarschäden für Räume und IT-Systeme

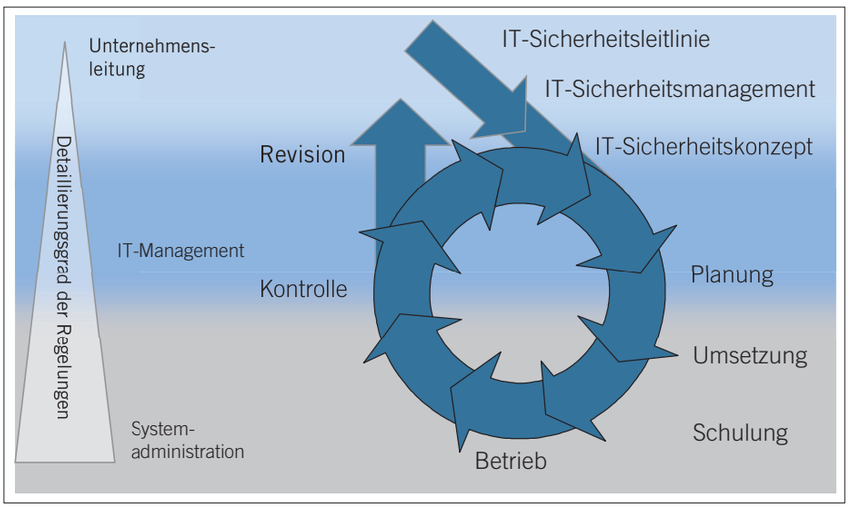
Einbrecher und Diebe haben oft allzu leichtes Spiel. Über Nacht gekippte Fenster, unverschlossene IT-Räume, unbeaufsichtigte Besucher oder im Auto zurückgelassene Notebooks bieten ungebetenen «Gästen» vielfältige Möglichkeiten. Schwerer als der Verlust von Hardware durch Diebstahl oder Vandalismus wiegt im Allgemeinen jedoch der Verlust der sich darauf gespeicherten Daten. Diese sind, wenn überhaupt, nur mit grossem Aufwand wiederzubeschaffen. Ausserdem droht die Gefahr, dass der Dieb vertrauliche Daten missbraucht. Katastrophen wie Brände oder Überschwemmungen sind zwar recht seltene Ereignisse, aber wenn sie eintreten, sind die Folgen meistens fatal. Brandschutzmassnahmen, Schutz vor Wasserschäden und die Sicherstellung der Stromversorgung sollten daher als wichtiger Bestandteil der IT-Sicherheit verstanden werden.

Das Sicherheitsaudit als Ausgangslage zur Verbesserung der IT-Sicherheit

Die schlimmsten Risiken sind jene, die nicht als solche erkannt werden, weil keine entsprechenden Sicherheitsmassnahmen getroffen werden. Diese Risiken können dem Unternehmen daher erhebliche Schäden zufügen. Man bedenke, dass der Kapitän der Titanic einmal sagte: «Ich kann mir nichts vorstellen, was dieses Schiff zum Sinken bringt. Ich kann mir keine Katastrophe vorstellen, die diesem Schiff zustossen könnte.»
So, wie das Treuhandunternehmen Revisionen für ihre Kundschaft anbieten, um die Einhaltung der Richtlinien und Gesetze sowie der Integrität der Buchhaltung sicherzustellen, so durchleuchtet ein IT-Sicherheitscheck das Unternehmen nach Schwachstellen in der Informationsverarbeitung.
Das Audit betrachtet sämtliche Bereiche der Informationsverarbeitung wie Organisation, Personal, Prozesse, Datensicherung, Virenschutz, Gebäude- und IT-Infrastruktur, Telekommunikation, Netzwerke und vieles mehr. Das Resultat des Audits ist ein Audit-Report, bestehend aus einer detaillierten Situationsanalyse sowie einer Liste alle Versäumnisse und entsprechenden Massnahmen. Der den unternehmensspezifischen Bedürfnissen entsprechend priorisierte Massnahmenkatalog ermöglicht die sofortige und nachhaltige Umsetzung der Sicherheitsmassnahmen. Die Umsetzung kann durch den bevorzugten IT-Partner erfolgen, mit Vorteil jedoch unter der Führung eines IT-Sicherheitsspezialisten.

IT-Sicherheit als steter Prozess

Die allermeisten Unternehmer besitzen eine Unternehmensleitlinie, mit welcher die Geschäftsstrategie und -ziele festgelegt werden. Von dieser Unternehmensstrategie muss auch eine IT-Sicherheitsstrategie abgeleitet werden. Damit wird bereits grob umschrieben, welche Unternehmensteile im Bereich der IT unternehmenskritisch sind und somit besondern Schutz bedürfen. Ausgehend von dieser Sicherheitsleitlinie lassen sich die IT-Sicherheitsmassnahmen definieren, bewerten (Risikobereitschaft) und letztendlich ihrer Priorität entsprechend umsetzen.
Um das angestrebte Sicherheitsniveau dauerhaft zu gewährleisten, müssen die implementierten IT-Sicherheitsmassnahmen laufend à jour gehalten werden. In wohl kaum einem anderen Bereich «veraltet» ein einmal etabliertes Sicherheitsniveau so schnell wie im dynamischen IT-Umfeld. Vor allem Erkenntnisse aus sicherheitsrelevanten Zwischenfällen, Veränderungen im technischen oder organisatorischen Umfeld sowie Änderungen von Sicherheitsanforderungen bzw. neue Bedrohungen erfordern Anpassungen der bestehenden IT-Sicherheitsmassnahmen. Zudem müssen für die Mitarbeiter entsprechende Sensibilisierungskurse für die IT-Sicherheit sowie Schulungen für die Nutzung der IT angeboten werden. Nur mit regelmässigen Sicherheitsaudits kann gewährleistet werden, dass diese nötigen Anpassungen auch tatsächlich durchgeführt werden!



Der IT-Sicherheitsprozess muss von der Unternehmensleitung angestossen und regelmässig kontrolliert werden.

Der unternehmerische Nutzen von IT-Sicherheit

Jeder gute Unternehmer kennt seine Risiken, bewertet diese und trifft geeignete Massnahmen. Das Risiko-Portfolio einer Unternehmung besteht jedoch nicht nur aus Risiken, die sich aus der unternehmerischen Tätigkeit ergeben, sondern auch Risiken im Bereich der IT. Der unternehmerische Wert von IT-Sicherheit kann somit daran gemessen werden, wie viel einem Entscheidungsträger die Umsetzung der Massnahmen wert sind.
Des Weiteren dürfen auch die folgenden, aus einem gut durchdachten und in der Praxis «gelebten» IT-Sicherheitskonzept resultierenden Effekte nicht unbeachtet bleiben:

- Wird Kunden gegenüber mit klaren Sicherheitsrichtlinien aufgetreten – zum Beispiel mit Vorgaben bezüglich elektronischen Datenaustauschs – so generiert dieses Vorgehen in der Regel zusätzliches Vertrauen und festigt damit die Partnerschaft. Generell kann gesagt werden, dass nachgewiesene IT-Sicherheit bei Kunden und Geschäftspartnern Vertrauen schafft und von diesen zunehmend auch eingefordert wird.
- Falls ein Unternehmen von Basel II-Akkord betroffen ist, kann sich die Kreditwürdigkeit u. U. verbessern, sofern die internen Risiken – und dazu gehören auch die IT-Risiken – möglichst gering gewichtet werden.
- IT-Systeme sind gut dokumentiert, was System-Administratoren die tägliche Arbeit stark erleichtert. Im Schadenfall können Daten schnell wieder beschafft und dem Benutzer verfügbar gemacht werden, was den Mehraufwand in vernünftigen Grenzen hält. Ausserdem kennen sich Administratoren und Anwender besser mit ihren Systemen aus und arbeiten dadurch effizienter.
- Last but not least die Arbeitsqualität steigt. Gelebte IT-Sicherheit fördert eine Unternehmenskultur, in der verantwortungsbewusstes Handeln, Kundenorientierung und die Identifikation mit den Unternehmenszielen fest verankert sind.

Fazit

IT-Sicherheit ist ein Thema, dem sich kein Unternehmer verschliessen darf. Insbesondere in Branchen, in denen täglich mit sensitiven Daten Dritter umgegangen wird, muss dem Thema besondere Aufmerksamkeit gewidmet werden. Dabei ist es weniger wichtig, alles zu tun, was möglich ist, sondern vielmehr ganz bewusst bestimmte Risiken einzugehen. Ein Security-Audit fördert die spezifischen IT-bedingten Risiken einer Unternehmung zu Tage und bildet so für relativ wenig Geld die Basis für ein solides Risiko-Management. ■

IT-Sicherheit im Unternehmen ist Chefsache! Handeln sie, bevor es zu spät ist!