Notfallpläne im Falle eines Informatiksupergau sind vielerorts überhaupt nicht vorhanden!

Studien zeigen auf, dass mehr als 40% der mittleren und grossen Unternehmen entweder gar keine oder nur unzureichende Notfallpläne im Falle eines Informatiktotalausfall besitzen. Vielfach sind vorhandenen Notfallpläne auch veraltet und deshalb im Falle eines Falles nicht mehr durchführbar.
Sicherheit im Unternehmen ist keine isolierte Komponente mehr, sondern ein unternehmens-umspannendes Konzept. Jeder Mitarbeiter und jedes eingesetzte informationsverarbeitende System im Unternehmen ist ein Teil des Ganzen. Es geht sogar darüber hinaus, wenn man global verteilte Zusammenarbeit, Outsourcing oder Application Service Providing mit in die Betrachtung einschliesst. Leider sehen das viele Unternehmen anders. Der Stellenwert von It-Sicherheit wird vielfach gleichrangig mit Informationsverarbeitung gestellt oder als lästiges Ãœbel abgetan, nur in wenigen Unternehmen wird dies als vorrangiges Ziel eingestuft. Da kann es nicht wundern, wenn die meisten Unternehmen gerade einmal der kleinster Teil der IT-Ausgaben für Sicherheit verwenden. Zu ändern ist dies nur durch eine Annahme dieser Aufgabe durch die Geschäftsleitung unterstützt durch den Verwaltungsrat. Die Verantwortung für die ausreichende Sicherheit des Unternehmens kann nicht delegiert werden, sie verbleibt in den Händen der Unternehmensleitung und ist deshalb als Chefsache zu interpretieren. Sie muss den Auftrag zur Erstellung eines individuellen Sicherheitskonzepts erteilen und die Durchsetzung, Einhaltung und implementieren des Konzepts unter Einbeziehung der notwendigen Expertisen gewährleisten. Anhand der Gefahren welche von kriminellen Elementen aus gehen, muss bei den Informatikverantwortlichen das Sicherheitsdenken sensibilisiert werden, ein Bewusstsein für die Problematik anhand konkreter Gefährdungen geweckt werden um ein Sicherheitskonzept zu entwickeln, welches zugegebenermassen ein vertieftes Know How erfordert und dementsprechend auch Geld kostet.

Gefahren in der Informationstechnik sind allgegenwärtig

Unternehmen und deren Beschäftigten sind mittlerweile Mitglieder von mitunter globalen Supply- und Value-Chains, deren Existenz und ihre hohe Dynamik ausschliesslich der leistungsfähigen Informations- und Kommunikationstechnik zu verdanken ist. Die Vernetzung durch das Internet, die Dezentralisierung und Virtualisierung von Unternehmen und die damit verbundenen Leistungen und Chancen für elektronisches Wirtschaften werden von den Teilnehmern der digitalen Welt gerne in Anspruch genommen und sind mittlerweile auch nicht mehr wegzudenken. Dabei vergessen einige schnell die wachsenden Risiken, die zum einen erst durch die Technologie selbst entstehen und zum anderen Risiken, die durch die Technologien verstärkt werden. Hacker greifen gerne auf im Internet frei verfügbare Tools zurück mit denen es immer einfacher ist, Firewalls zu umgehen oder zu überlisten. Für die Erzeugung von Viren werden ebenfalls im Internet fixfertige Tools angeboten. Eins haben fast alle diese "Erzeugnisse" gemeinsam, sie nutzen Sicherheitslücken und bekannte Schwachstellen von Datennetzkomponenten und Softwareprodukten aus. Kommt es zu massiven Bedrohungen durch Ereignisse wie etwa verteilte Angriffe (DDoS, Distributed denial of service), die zum vorübergehenden schliessen der Websiten von Unternehmen geführt haben, ist die Bestürzung und die Ratlosigkeit bei vielen Teilnehmern des Internet zumindest zeitweilig gross. Leider ist aber die nachhaltige Wirkung von solchen Ereignissen dennoch gering. Solange man nicht als Betroffener einschlägige Erfahrungen mit hohen wirtschaftlichen Verlusten hinnehmen muss, ist wohl die Bereitschaft eigene Schutzmassnahmen zu ergreifen wenig ausgeprägt. Dies bestätigen auch unlängst gemachte Studien. An dieser Situation sollte sich allerdings schnell etwas ändern. Einer der Grundvoraussetzungen für das Gelingen dieses vorhaben ist es, sich über die Bedrohungslage welches das Unternehmen betrifft, aufzuklären und die Mitarbeiter dahingehend zu sensibilisieren. Eine weiteres muss ist es dass, das Management mit gutem Beispiel vorangeht, will man die Strukturen in den Unternehmen ändern. Die meisten Unternehmen haben die Vernetzung stark vorangetrieben. Ohne Internetanbindungen wären viele Geschäftsprozesse heute nicht mehr abwickelbar. Mit Application Service Providing beispielsweise werden immer mehr Anwendungen, die früher im eigenen Rechnernetz oder dem Rechenzentrum liefen, von einem Serviceprovider erledigt. Mit der notwendigen Offenheit des Unternehmensnetzes kommen aber zeitgleich neue informationstechnische Bedrohungen auf das Unternehmen zu, die in dieser Form bislang nur begrenzt existierten. Die Bedrohungen lassen sich in passive und aktive Angriffe im Netz sowie unbeabsichtigte Gefährdungen unterteilen.

Risikofaktor Mensch

Der Umgang mit Computersystemen und immateriellen Daten ist für den Menschen gemessen an seiner Jahrtausende alten Geschichte immer noch recht neu. Daher ist ein Bewusstsein für die Risiken und die Gefahren im Umgang damit weit weniger ausgeprägt als mit Gütern aus der materiellen Welt. Zwar lassen sich viele Bedrohungen mit technischen Verfahren eingrenzen, aber gegen menschliches Versagen können sie häufig nicht viel ausrichten. Psychologische Tricks werden gerne benutzt um soziale Angriffe auf Wissensträger durchzuführen. Das erbeutete Wissen lässt sich dann für die folgenden Angriffe auf technischer Ebene hervorragend nutzen. Leider sind zu viele Menschen zu leichtgläubig und

fallen auf einfachste Täuschungen hinein. Erfahrungen zeigen, dass die meisten erfolgreichen Angriffe auf Informationen des Unternehmens durch die Ausnutzung von Löchern in organisatorischen Regeln erst ermöglicht wurden. Beispielsweise werden Benutzerpasswörter allzu leicht an andere Personen weitergegeben. Auch um die Effizienz seiner Wartungsarbeiten an Arbeitsplatzrechnern zu steigern, lassen sich manche Netzwerkadministratoren die Passwörter von Mitarbeitern geben. Dies kann sich im Fall einer Ab- oder Anwerbung des Administrators durch Konkurrenten verheerend auswirken! Auch die Bequemlichkeit von Nutzern lässt sich ausgezeichnet für Attacken nutzen. So werden häufig bewusst Sicherheitsfunktionen umgangen, da sie das schnelle Arbeiten verhindern oder ein Passwort für viele unterschiedliche Systeme verwendet. Aus diesem Grund ist die organisatorische Sicherheit eine ganz wesentliche Komponente eines Sicherheitskonzepts für ein Unternehmen.

Die Ursache Mensch ist für die meisten Bedrohungen selbst verantwortlich. Bewusst, also mit kriminellem Hintergrund, und unbewusst werden Schadprogramme verbreitet, Informationen ausgespäht, verändert oder missbraucht. Oder verfügbare Programme und Systeme werden fehlerhaft entwickelt oder implementiert und fallen deshalb aus. Aber selbst wenn Systeme an sich nicht fehlerhaft sind, kann es zu Ausfällen kommen, wenn Systeme miteinander verknüpft werden, die darauf hin nicht konzipiert wurden. Viele Altlasten aus den Anfangszeiten der Programmierung (Legacy-Codes) sind noch heute im Einsatz und werden in einigen Bereichen auch auf absehbare Zeit nicht abgelöst. Das Jahr2000-Problem ist in diesem Zusammenhang noch allen bekannt. Zahlreiche Unternehmen erbringen Leistungen zur Grundversorgung der Bevölkerung, beispielsweise Banken, Telefongesellschaften, Energiegesellschaften oder die Stellen zur Sicherung vom Luft- und Verkehrsnetz. Ihr Ausfall oder Fehlfunktion stellt, selbst bei zeitlicher Begrenzung, eine grosse Bedrohung für die Gesellschaft dar. In diesem Zusammenhang spricht man von kritischen Infrastrukturen. Diese Unternehmen sollten noch weitergehende Massnahmen ergreifen, um ihr Funktionieren zu gewährleisten. Die zunehmende Vernetzung lässt den weltweiten Wettbewerb und Kostendruck zunehmen. Unternehmen dürfen es sich nicht leisten, die Sicherung des Unternehmenswissens, welches fast ausschliesslich nur noch elektronisch und in den Köpfen der Mitarbeiter archiviert ist, dem Zufall zu überlassen. Jedes Unternehmen braucht ein Sicherheitskonzept, welches sich dynamisch an die immer ändernden Herausforderungen anpasst. Dies ist eine strategische Aufgabe und ist deshalb die Aufgabe der Geschäftsleitung!

Sicherheitskonzept und Massnahmenkatalog

Wie bei Einsatz jeder neuer Technologie, entstehen mit ihr auch neue Bedrohungen. Die Bedrohungen können systemimmanent sein oder durch bewusste und unbewusste Handlungen herbeigeführt werden. It-Sicheherheit beschäftigt sich mit der Gefährdungs- und Risikoanalyse und erarbeitet Massnahmen, um den Bedrohungen zu begegnen und die Risiken der Anwendung von ITK-Technologien zu minimieren. In einer Bedrohungsanalyse werden alle vorstellbaren Bedrohungen ermittelt, die Schäden verursachen könnten. Die Bedrohungen werden verschiedenen Ebenen zugeordnet: Der rechtlich-wirtschaftlichen, der organisatorisch-sozialen, der logischen und der physischen Ebene. An die Bedrohungsanalyse schliesst sich eine Risikoanalyse an, die die Häufigkeit und Höhe von Schäden den jeweiligen Bedrohungen zuordnet. Der Geschäftsführung obliegt es dann, eine Risikopolitik festzulegen und in ihren unternehmerischen Entscheidungen die jeweiligen Risikokomponenten zu berücksichtigen. Das Ergebnis ist dann ein Sicherheitskonzept, welches den konkreten Risiken Massnahmen entgegenstellt, die das Risiko auf ein annehmbares Niveau reduzieren. Die gewählten Schutzmassnahmen, bestehend aus technischen, organisatorischen und juristischen Komponenten, sollten die Differenzierung des Schutzklassenkonzepts übernehmen. Unternehmen, die über keine oder nur wenige Hochqualifizierte- Mitarbeiter im Bereich Sicherheit verfügen, sollten bei der Entwicklung eines Sicherheitskonzeptes unbedingt auf externe kompetente Beratung zurückgreifen. Nur so kann sichergestellt werden, dass die Analyse des Zustands und die ausgesprochene Empfehlung und die Umsetzung des Sicherheitskonzepts dem "State of the Art" entspricht, der sich bekanntermassen im Internetbereich täglich weiterentwickelt.

IT-Sicherheit auf dem Prüfstand

Viele Anwender und Hersteller wollen wissen, wie technisch sicher tatsächlich ihre eingesetzten oder entwickelten Systeme sind. Dafür wird ein Massstab benötigt, mit dem man das erreichte Mass an Sicherheit evaluieren, dokumentieren und vergleichen kann. Aber auch, um beispielsweise bei der Entwicklung von sicheren Systemen zu Beginn an schon festlegen kann, welches Sicherheitsmass erreicht werden muss. Solche Sicherheitsmassstäbe sind in unterschiedlichen Kriterienwerken für sichere Informationstechnik festgelegt. In Europa werden vor allem die ITSEC-Kriterienwerke (Information Technology Security Evaluation Criteria für die Bewertung der Sicherheit von Systemen in der Informationstechnik verwendet, die gemeinsam von Sicherheitsagenturen aus den USA, Kanada, Grossbritannien, Frankreich, Deutschland und Niederlanden entwickelt wurden. Die ITSEC Kriterien umfassen in erster Linie die Bewertung technischer Sicherheitsmassnahmen. Organisatorische, personelle und administrative Massnahmen werden zwar berücksichtigt, stehen aber nicht im Vordergrund. Die Kriterien sind so abstrakt gehalten, dass sowohl Hard- als auch Software damit evaluierbar ist. Als Ausprägung des Masses der erreichten Sicherheit definieren die ITSEC Kriterien sieben Stufen (E1 bis E7) der Vertrauenswirklichkeit, wobei E1 die geringsten und E7 die höchsten Anforderungen definiert. Die Stufe gibt an, wie korrekt die geprüfte Funktion implementiert wird. Bereits in der Entwicklung eines Produktes muss dazu beispielsweise die Funktion getestet, methodisch getestet, teilanalysiert,

semiformal analysiert oder sogar formal analysiert und getestet sein. Je mehr Grad an Korrektheit erwartet wird, desto teurer und aufwendiger wird die Entwicklung und die darauf folgende Evaluierung. Die Korrektheit allein sagt noch nichts über die Stärke der Sicherheitsfunktion, der Mechanismenstärke aus. Diese wird getrennt bewertet und mit einem Prädikat "einfach", "mittel" oder "hoch" definiert. Bei den Common Criteria ist die Herangehensweise leicht unterschiedlich. Bei ihrer Verwendung wird zunächst ein generisches Schutzprofil für eine bestimmte Art Anwendung entwickelt. In diesem werden die durch die Implementierung zu erreichende Vertrauenswirklichkeit und Mechanismenstärke festgelegt. Anschliessend können alle nach dem Schutzprofil entwickelten Produkte hiernach evaluiert und verglichen werden.