Das IT-Sicherheitskonzept

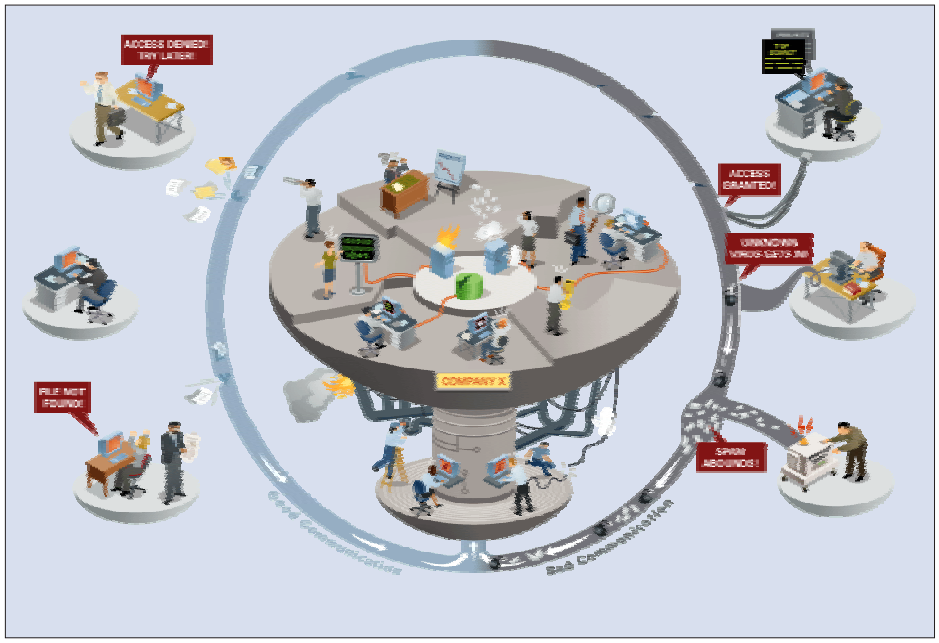
Die Grundlagen für jede IT-Umgebung sind ein IT-Konzept und darauf aufbauend ein IT-Sicherheitskonzept. In vielen Firmen findet man ein IT-Konzept, doch das ebenso wichtige Sicherheitspapier fehlt. Dieser Beitrag soll zeigen, wie ein IT-Sicherheitskonzept geplant und erstellt werden kann.

VON ANDREAS WISLER*

Das IT-Sicherheitskonzept beschreibt die notwendigen Massnahmen zur Realisierung und Aufrechterhaltung des für das Unternehmen angemessenen, definierten Sicherheitsniveaus. Darauf basierend kann im Unternehmen ein angemessenes Sicherheitsniveau erreicht und bei konsequenter Durchsetzung der Massnahmen auch gehalten werden. Wichtig ist: Das IT-Sicherheitskonzept betrifft alle Stufen. Die Geschäftsführung ist also genau gleich beteiligt, wie die IT-Leitung und die Mitarbeiter.

Damit ein IT-Sicherheitskonzept erstellt werden kann, müssen vier Fragen beantwortet werden:

1. Was will ich schützen?
2. Wogegen soll ich mich schützen?
3. Wie kann ich diesen Schutz erzielen?
4. Kann ich mir diesen Schutz leisten?



Schutzbedarf

Die erste Frage gilt dem Schutzbedarf. Was will ich schützen? Die drei Schutzziele Verfügbarkeit, Verbindlichkeit und Vertraulichkeit helfen, diese Frage zu beantworten. Die Verfügbarkeit gibt an, welche Systeme, Prozesse, Abläufe und Personen für welche Situation zur Verfügung stehen müssen. Wie verbindlich die Resultate oder Angaben sind, wird unter dem Begriff Verbindlichkeit sichergestellt. Die Vertraulichkeit schützt die Daten vor fremden Blicken.

«Der wichtigste Punkt bei der Umsetzung sind die Verantwortlichkeiten.»

Drei Beispiele dazu:

► Cockpit eines Airbus: Im Cockpit eines Airbus ist es von zentraler Bedeutung, dass die Instrumente immer verfügbar sind und die Angaben auf den Anzeigen korrekt, also verbindlich sind. Die Daten sind jedoch nur minimal vertraulich. Aus diesem Grund werden die wichtigsten Anzeigen in einem Flugzeug in doppelter oder gar dreifacher Ausführung angebracht. Auch wenn ein Instrument ausfällt, kann immer noch an die flugrelevante Information gelangt werden.

► Online-Bank: Bei einer Online-Bank ist dem Kunden wichtig, dass die Vertraulichkeit jederzeit gewährleistet ist. Nur ich darf meine Daten sehen. Unvorstellbar, wenn diese Angaben in die Hände Dritter gelangen oder die Informationen abgefangen werden. Die Verfügbarkeit ist aus Sicht des Images einer Bank ebenfalls wichtig. Das Vertrauen in eine Bank schwindet, wenn die Kunden während mehrerer Tage nicht mehr an die Konten gelangen. Die Verbindlichkeit der Angaben nimmt hier nur eine nebensächliche Position ein. Der Kontoauszug Ende des Monats ist das verbindliche Papier und wird daher auch im Kleingedruckten geregelt.

► Kasse eines Parkhauses: Bei einer Kasse ist die Verbindlichkeit das wichtigste Argument. Es freut sich niemand, der nach korrekter Bezahlung das Parkhaus doch nicht verlassen kann, weil die Barriere unten bleibt. Sollte dann doch einmal die Kasse nicht verfügbar sein, steht auch die Schranke offen. Es stört sich auch niemand, wenn der Hintermann den zu bezahlenden Betrag mitlesen kann (Vertraulichkeit).

Wogegen muss ich mich schützen?

Ein Unternehmen muss sich klar sein, welche Gefährdungen einwirken können und ab welchem Punkt ein Schaden bedrohlich wird. Hier gilt es verschiedene Szenarien und die Folgen abzuschätzen. Dies können beispielsweise Stromausfall, Wassereinbruch, Mitarbeiteraustall, Systemabsturz, Viren, Hacker, Sabotage und viele mehr sein.

Massnahmenauswahl

Aus dem Schutzbedarf und der Risikoanalyse leiten sich Massnahmen ab. Welche Massnahmen davon sind überhaupt möglich? Damit auch verbunden, welche Gefährdungen kann eine einzelne Massnahme abdecken? Hat diese allenfalls Einfluss auf andere Gefährdungen oder Massnahmen? Welche Bereiche werden zusätzlich tangiert? Je nachdem, welche Bereiche abgedeckt werden, sind mehr Personen – vielleicht sogar Externe – involviert oder es müssen verschiedene Prozesse angepasst werden. Eine zentrale Frage ist auch der Nutzen. Was bringt es mir, wenn ich eine Massnahme umsetze? Habe ich anschliessend die Ressourcen, diese Massnahme aufrechtzuerhalten? Als ein Stichwort eignen sich Intrusion-Detection-Systeme. Die Flut an Daten wird hier oft unterschätzt, und die Kontrolle dieser wird nur unregelmässig durchgeführt. Wenn diese jedoch nicht ausgewertet werden, ist das System nutzlos.

Sobald Massnahmen für die einzelnen Bereiche definiert wurden, gilt es diese zusammenzufassen und Synergien zu finden.

Wirtschaftlichkeit

Schlussendlich dreht sich alles um das Geld. Kann und will ich mir diesen Schutz leisten? Hier scheitern die meisten Projekte. Doch es ist wichtig, anzuschauen, welchen Schaden eine Gefährdung anrichten kann. Teilen Sie die Auswirkungen in Kategorien von niedriger bis mittlerer Schaden, hoher Schaden und sehr hoher Schaden ein. Dort, wo der Schaden am grössten wird, sollten die ersten Massnahmen stattfinden.

Es stellen sich nun die Fragen nach den Restrisiken. Was bleibt übrig, wenn ich eine Massnahme umgesetzt habe? Wie hoch ist die Eintrittswahrscheinlichkeit für die restlichen Gefährdungen? Diese Frage ist nur sehr schwer zu beantworten, da Erfahrungswerte fehlen.

«Nur was bekannt ist, wird auch gelebt.»

Vorgehen

Mit den Antworten auf diese vier Fragen kann das weitere Vorgehen definiert werden. Die Resultate sind zu bewerten und detailliert auszuarbeiten. Damit verbunden sind die Kosten. Jedoch wird hier oft nur der materielle Aufwand angeschaut und die zeitliche Belastung vergessen. Meistens ist dieser Betrag viel höher. Mit der Auswahl der Massnahmen kann auch die Reihenfolge definiert werden. Welche Massnahmen sind zeitkritisch? Welche Massnahmen lassen sich auch später noch realisieren? Hier lohnt es sich, Zeit zu investieren. Was sich zusammenlegen lässt, sollte auch gleichzeitig umgesetzt werden.

Der wichtigste Punkt bei der Umsetzung sind die Verantwortlichkeiten. Wer trägt die Verantwortung für eine Massnahme? Nur wer sich verpflichtet fühlt, wird auch das Zepter in der Hand halten.

Gleichzeitig mit der Umsetzung sind die begleitenden Massnahmen. Die Schulung und Sensibilisierung von Mitarbeitern ist wichtig. Die Mitarbeiter müssen früh genug auf die Umstellungen vorbereitet werden, um einem möglichen Widerstand vorzubeugen.

Inhaltsverzeichnis eines IT-Sicherheitskonzeptes

Unten stehend ist ein mögliches Inhaltsverzeichnis eines IT-Sicherheitskonzeptes abgebildet:

Grundlage, Zweck

Die Einleitung beschreibt die Grundlagen der Firma, die Infrastruktur und die vorhandenen Mittel (Maschinen, Mitarbeiter, Wissen). Welchen Zweck erfüllt die Firma? Welche Stellen sind involviert?

Anforderungen (Funktionalität, Sicherheit, Benutzer, Administration)

Die Anforderungen sind oft mannigfaltig. Jede Stelle oder Position hat andere Ansprüche an die Umgebung und Mittel. Daher ist es sinnvoll, die Funktionen und Prozesse über alle Stufen aufzuschreiben und die wichtigen Etappen festzuhalten.

Mit den Anforderungen der Anwender leiten sich auf der Geschäftsseite die Anforderungen an die Sicherheit ab. Es ist wichtig, beide Seiten gegenüberzustellen und ein geeignetes Mittelmass zu finden. Die Benutzer sollen nicht zu stark in ihrer Arbeit eingeschränkt werden, jedoch sollen die *Geheimnisse* einer Firma optimal geschützt sein.

Wichtig sind auch die Anforderungen der Administratoren. Sie sitzen in der Zwickmühle zwischen Wartung und Unterhalt sowie der optimalen Sicherheit.

Sicherheitsorganisation

Zuständigkeiten: Die Sicherheit gehört in den Zuständigkeitsbereich der Geschäftsleitung. Die Verantwortung kann gemäss Gesetz nicht nach unten delegiert werden. Jedoch können weitere Stellen bestimmt werden, die für (Teil-) Bereiche zuständig sind und gegenüber der Geschäftsführung Bericht ablegen.

► Rahmen für die Informationssicherheit: Das IT-Sicherheitskonzept muss von der Geschäftsleitung initiiert werden. Die Mitarbeiter (meistens die IT-Leitung) erstellen Anforderungen an die Umgebung und schlagen Lösungen vor. Diese werden durch die Geschäftsleitung genehmigt. Gleichzeitig sollte festgelegt werden, wann eine Überprüfung stattfinden soll.

► Pflege und Wartung des Sicherheitskonzepts: Die Situation in der IT wechselt ständig. Auch das Umfeld der Firma ändert sich sehr schnell. Da ist es wichtig, dass das IT-Sicherheitskonzept gepflegt und den veränderten Bedingungen angepasst wird. Der Rahmen für diese Arbeiten wird in diesem Kapitel festgehalten.

Sicherheit beim Personal

► Stellenbeschreibung und Rekrutierung: Dieser Bereich gehört in das Ressort des Personalleiters. Für jede Stelle muss eine Beschreibung vorhanden sein. Mit dieser Beschreibung können Gruppen (z.B. im Active Directory) definiert und die damit verbundenen Rechte genau ausgearbeitet werden. Gleichzeitig helfen diese Unterlagen, nötige Rekrutierungen schnell durchführen zu können.

► Vertraulichkeitsvereinbarung: Informationen der Firma gehören auch der Firma und stellen das Potenzial und den wirtschaftlichen Vorteil gegenüber Mitbewerbern dar. Dieses Wissen muss geschützt werden. Alle Mitarbeiter werden schriftlich zur Vertraulichkeit verpflichtet. Hier muss auf die gesetzlichen Rahmenbedingungen (Schutz der Privatsphäre, Überwachung des Arbeitsplatzes) geachtet werden.

► Mitarbeiterausbildung in Sicherheitsfragen: Wie bereits erwähnt, nur was bekannt ist, kann auch gelebt werden. Die Mitarbeiter sind in regelmässigen Abständen zu sensibilisieren. Wichtig ist es jedoch, die Abstände nicht zu kurz zu definieren, da ansonsten eine Gleichgültigkeit entstehen kann. Als idealer Abstand ist ein halbes Jahr vorzusehen. Aktuelle Ereignisse, Lösungen sowie Tipps und

Tricks garantieren ein abwechslungsreiches Programm, das bei allen in Erinnerung bleibt.
► Reaktion auf sicherheitsrelevante Ereignisse und Schwachstellen: Wie soll man auf sicherheitsrelevante Ereignisse reagieren? Sollte ein Ereignis eintreten, sollte bekannt sein, wie man mit diesem umgehen will. Dies ist auch bei Patches von Vorteil. Steht eine Testumgebung zur Verfügung, damit der neue Patch getestet werden kann? Falls ja, sollte dieser schnellstmöglich ausgiebig getestet und anschliessend in die Produktion übertragen werden.

Physische Sicherheit
► Sicherheitsbereiche: Diese müssen definiert werden. Der Serverraum ist ein solcher Bereich, der nur einem bestimmten Personenkreis zugänglich sein darf. Der Schutzbedarf leitet sich aus diesen Bereichen ab (Klimatisierung, Alarmierung, Umgang mit Vorfällen).
► Verkabelung, Wireless LAN: Die Verkabelung gehört ebenfalls in die physische Sicherheit. Kabel sollten nicht durch *fremde* Gebiete geführt werden, um ein Abhören zu verhindern. Neue Gefährdungen durch Wireless-Geräte erhöhen die Gefahr von Mithörern. Vorkehrungen durch Verschlüsselungstechniken bieten Abhilfe.

Betrieb von Systemen und Netzwerken
► Operative Verfahren und Aufgaben: Das Daily-Business der Administratoren gehört ebenfalls in das IT-Sicherheitskonzept. Welche Dienste und Protokollierungen sind regelmässig zu kontrollieren? Welche Schritte leiten sich bei Vorfällen ab? Das Verfahren gehört in dieses Kapitel.
► Systemplanung und -abnahme: Neue Systeme sind auf die Verträglichkeit mit den bestehenden Mitteln zu testen. Ein Kontroll- und Abnahmeverfahren hilft, alle wichtigen Punkte zu erfassen.
► Systemverwaltung: Die Systeme sind regelmässigen Veränderungen ausgesetzt (Patches, Updates, neue Versionen). Die Verwaltung dieser muss vorgängig definiert und festgehalten werden.
► Umgang mit Datenträgern (Datenschutz): Datenträger wie Disketten, CD-ROMs und Speicherkarten sind eine einfache Möglichkeit, Daten zu transportieren. Ebenso einfach ist es, unerlaubt Daten zu transportieren. Der Umgang mit diesen Mitteln ist festzuhalten (z.B. im Mitarbeiterreglement, allenfalls sind technische Möglichkeiten vorzusehen).
► Internet: Das Internet ist eine ideale Informationsquelle. Ebenso leicht ist es, unerwünschte Software einzuschleusen. Daher ist auch der Internetzugang einzuschränken (technisch und organisatorisch). Die gewählten Massnahmen sind festzuhalten und zu kommunizieren.
► Schutz gegen böswillige Software (Viren): Viren sind immer eine ernst zu nehmende Gefahr. Diese verbreiten sich innerhalb weniger Stunden rund um die Welt. Der Schutz vor diesen Übeltätern muss durch ein mehrstufiges Netz sichergestellt werden.
► Sicherheit beim elektronischen Datenverkehr oder Handel: Handelsbeziehungen finden vermehrt elektronisch statt. Der Schutz dieser Verbindungen ist ebenso festzuhalten.

Zugriffskontrolle
► Benutzer Administration: Dieser Punkt behandelt die Art der Identifikation, der Kontrolle und der Administration der Benutzer (Gruppen, Rechte, Einschränkungen).
► Verantwortung der Benutzer: Die Benutzer sind oft das schwächste Glied, daher sind diese in die Verantwortung zu ziehen (Umgang mit Passworten und Geräten).
► Betriebssystem-Zugriffskontrolle: Wie wird der Zugriff auf das System geregelt? Wie werden die Zugriffe kontrolliert? Dies sollte hier festgehalten werden.
► Anwendungs-Zugriffskontrolle: Analoges gilt für die einzelnen Anwendungen. Welchen zusätzlichen Schutz bieten diese? Und wie können diese Zugriffe kontrolliert werden? Wer ist für die Kontrolle verantwortlich?
► Einsatz mobiler Computer: Mobile Geräte sind sehr schwer zu kontrollieren, da sie oft unterwegs sind. Bevor sie jedoch an das Firmennetz angeschlossen werden, müssen verschiedene Kontrollen stattfinden (Patches, Virenpattern).

Unterhalt von Informationssystemen

► Kryptische Kontrolle (Verschlüsselung, Schlüsselverwaltung): Spezielle Anforderungen gelten der Verschlüsselung. Welche Schlüssel werden eingesetzt? Welche Gebiete decken diese ab? Was geschieht mit abgelaufenen Schlüsseln? Was, wenn ein Mitarbeiter die Firma verlässt? Diese Fragen sind von zentraler Bedeutung.
► Änderungswesen: Änderungen an Systemen und Abläufen sind schriftlich festzuhalten, beispielsweise in einer Art Logbuch.

Not-Organisation
Ein wichtiges Kapitel ist die Notfallvorsorge. Welche Mittel sind für einen eingeschränkten Betrieb notwendig? Gibt es Ausweichmöglichkeiten (andere Gebäude, Lieferanten- und Wartungsverträge)?

Einhaltung und Überprüfung der Aufgaben
► Konformität mit gesetzlichen Angaben: Überwachung ist erlaubt, jedoch nur anonymisiert. Dieser Teil des IT-Sicherheitskonzeptes beschreibt, wie dem Datenschutz Rechnung getragen wird.
► Überprüfung der Sicherheitspolitik und der technischen Konformität: Regelmässige Überprüfungen durch interne und externe Stellen gewährleisten, dass das Konzept aktuell und komplett ist. Die Bedingungen für derartige Kontrollen sind vor dem Audit festzuhalten.

Anhänge
► Gefährdung und Risikoanalyse (inkl. Restrisiken)
► Informatik-Strategie und -Organisation
► Betrieb der Informatik-Struktur (Einleitung, Zielsetzung, Betrieb und Support, Sicherheit und Überwachung sowie Genehmigung)
► Nutzung von PC, Netzwerk und Online-Diensten
► Externe Nutzung von Hard- und Software
► Backup-Konzept
► Backup-Plan
► Firewall-Konzept
► Akzeptierte Ausfallzeiten und Not-Organisation
► Beurteilung der Informatik-Sicherheit

Der Anhang enthält weitere Unterlagen zum Betrieb, der Nutzung von Informatikmitteln sowie Backup und Firewall. Diese Unterlagen sollten nicht direkt in das IT-Sicherheitskonzept integriert, sondern nur via Verknüpfungen eingebunden werden.

Kontrolle

Mit der Planung und Umsetzung von Massnahmen ist es nicht getan. Eine regelmässige Kontrolle ist notwendig, um Abweichungen und veränderte Bedingungen zu erkennen und Anpassungen zu treffen. Auch hier gilt es Verantwortlichkeiten und Rechte festzuhalten, damit dies in periodischen Abständen passiert. Ein externer Berater kann hier ebenfalls neue Sichtweisen und Möglichkeiten aufzeigen.

Sollte es dann zu Änderungen kommen, ist das Management mit einzubeziehen und sind Entscheide zu treffen. Alle Mitarbeiter müssen frühzeitig über die veränderten Situationen orientiert sein.

Zusammenfassung

Ein IT-Sicherheitskonzept ist nicht in einem Tag erstellt. Die Vorbereitungsarbeiten nehmen sehr viel Zeit in Anspruch. Doch diese Zeit lohnt sich. Massnahmen, die sich auf kritische Systeme auswirken, sollten anschliessend im ersten Schritt umgesetzt werden. Halten Sie fest, wer die Verantwortung für die Umsetzung und Kontrolle von Massnahmen trägt.

Während und nach der Umsetzung gilt es, diese Massnahmen zu kontrollieren, sei es durch externe oder interne Stellen.

Nur was bekannt ist, wird auch gelebt. Oft scheitert es an Kleinigkeiten. Daher schulen und sensibilisieren Sie alle Stufen, von der Geschäftsleitung bis zum Mitarbeiter. So führt ein Konzept zum Erfolg.

** Andreas Wisler ist Dipl. Ing. FH, Sicherheitsspezialist und Mitglied der Geschäftsleitung der GO OUT Production GmbH.* ■