Sicherheit ist Chefsache

IT-SECURITY Zehn einfache Schritte sorgen für einen minimalen Schutz gegenüber den Risiken der Informationsverarbeitung. Die Sorgfaltspflicht über die Einhaltung dieser Vorsichtsmassnahmen liegt bei der Geschäftsleitung und kann nicht delegiert werden.

WOLFGANG SIDLER

Ohne IT läuft nichts – das gilt selbstredend auch für die kleinen und mittleren Unternehmen der Schweiz. Ihre Produkte und Dienstleistungen basieren auf Qualität, Flexibilität und Innovationskraft.

Informationssicherheit ist daher eine strategische und nicht ausschliesslich eine technische Frage. Informationssicherheit kann nur wirkungsvoll und nachhaltig umgesetzt werden, wenn sie ein fester Bestandteil der Unternehmenspolitik ist und das IT-Sicherheitsmanagement organisatorisch im Unternehmen eingebunden wird.

Die Erkennung und Festlegung der kritischen Informationen für ein Unternehmen und die anschliessende Auswahl der geeigneten Massnahmen zur Informationssicherheit sind Führungsaufgaben, die sich nur eingeschränkt delegieren lassen. Damit die Informationssicherheit erfolgreich umgesetzt werden kann, ist die volle Unterstützung des Managements nötig.

Die Verantwortung für die Informationssicherheit liegt beim Management, welches die notwendigen Massnahmen initiieren und deren Umsetzung kontrollieren muss.

Management ist verantwortlich

Dabei gelten die folgenden Management-Grundregeln:

- Die Verantwortung für die Informationssicherheit liegt beim Management und kann nicht abgegeben werden. Es entscheidet über den Umgang mit den Risiken, stellt die notwendigen Mittel zur Verfügung und trägt das verbleibende Restrisiko.
- Informationssicherheit muss in alle Prozesse und Projekte integriert werden, bei denen Informationen verarbeitet und genutzt werden.
- Der Informationssicherheitsprozess muss vom Management überwacht werden.
- Für den IT-Betrieb und die Informationssicherheit müssen ausreichende Ressourcen bereitgestellt werden.
- Es müssen die organisatorischen Rahmenbedingungen für die Informationssicherheit geschaffen werden.
- Die Umsetzung muss wirtschaftlich sein. Informationssicherheit darf nicht mehr kosten als die damit erreichte Risikominderung.
- Die Informationssicherheit muss in sinnvoller Relation zum Schutzbedarf stehen (Angemessenheit).
- Die Schutzmassnahmen müssen realisierbar sein und dürfen die Sicherheitslage nicht verschärfen (Praktikabilität). Sie müssen nachweisbar Bedrohungen abwehren bzw. Risiken mindern (Wirksamkeit).
- Informationssicherheit darf die Geschäftstätigkeit nicht behindern und muss von allen als Notwendigkeit verstanden werden (Akzeptanz).
- Die IT-Sicherheitspolitik und die Strategie müssen in regelmässigen Abständen überprüft werden.

Die virtuellen Türen zum Unternehmen müssen sicher verriegelt sein.

Als Erstes muss in einem Unternehmen die Sicherheitspolitik festgelegt werden. Sie stellt grob die allgemeine Richtung der Informationssicherheit dar. Damit bestimmt die Unternehmensleitung, welchen Stellenwert sie in Sachen Sicherheit vertritt. Der Sicherheitsverantwortliche des Unternehmens und das Sicherheitskonzept unterstützen dabei die Geschäftsleitung in der Umsetzung der Strategie. Informationssicherheit betrifft ohne Ausnahme alle Mitarbeitende in einem Unternehmen. Jeder Einzelne kann durch verantwortungs- und qualitätsbewusstes Handeln und Verhalten Schäden vermeiden und zum Erfolg beitragen. Sensibilisierung für Informationssicherheit und entsprechende Schulungen der Mitarbeitenden sowie aller Führungskräfte sind daher eine Grundvoraussetzung für eine erfolgreiche Informationssicherheit.

Um Sicherheitsmassnahmen wie vorgesehen umsetzen zu können, müssen bei den Mitarbeitenden die erforderlichen Grundlagen vorhanden sein. Dazu gehört neben den Kenntnissen, wie Sicherheitsmechanismen bedient werden müssen, auch das Wissen über Sinn und Zweck von Sicherheitsmassnahmen. Auch das Arbeitsklima, gemeinsame Wertvorstellungen und das Engagement der Mitarbeitenden beeinflussen entscheidend die Informationssicherheit und steuern einen wichtigen Beitrag zu einer erfolgreichen und wirksamen Sicherheitskultur bei.

Mitarbeiter sensibilisieren

Werden Mitarbeitende neu eingestellt oder erhalten neue Aufgaben, ist eine gründliche Einarbeitung und Ausbildung notwendig. Hier empfiehlt es sich, den neuen Mitarbeitenden beim Eintrittstag kurz die Sicherheitspolitik mit den entsprechenden Weisungen vorzustellen. Wenn Mitarbeitende das Unternehmen verlassen oder sich ihre Zuständigkeiten verändern, muss dieser Prozess durch geeignete Sicherheitsmassnahmen begleitet werden (z.B. Entzug von Berechtigungen, Rückgabe von Schlüsseln und Ausweisen). Wichtig ist, dass die für die Informationssicherheit verantwortlichen Personen vorgestellt werden, damit die Mitarbeitenden bei Sicherheitsvorfällen schnell die entsprechenden Experten informieren können.

Vergessen Sie nicht, externe und temporäre Mitarbeiter entsprechend zu sensibilisieren und verlangen Sie von ihnen, dass sie eine Vertraulichkeitsvereinbarung beim Eintritt unterschreiben. Folgende Weisungen sind für ein Unternehmen zwingend notwendig:

- Umgang mit E-Mail;
- Umgang mit Internet;
- Umgang mit IT-Sachmittel;
- Umgang mit Passwörtern.

Experten an Bord holen

Das neue 10-Punkte-Programm ist einfach gehalten und Massnahmen können auch in einem kleinerern Unternehmen realisiert werden, ohne dass dafür grosse Kosten entstehen. Wo das spezifische Fachwissen in einem KMU nicht verfügbar ist, ist es ratsam, sich von einem externen Experten unterstützen zu lassen.

Wolfgang Sidler, Präsident, InfoSurance, Organisation für die Sicherheit der Informationsinfrastruktur in der Schweiz, und Inhaber Sidler Information Security, Hünenberg.

DIE 10 GOLDENEN REGELN

So verbessern Sie Ihre IT-Sicherheit

Regel 1: Erstellen Sie ein Pflichtenheft für IT-Verantwortliche
IT-Sicherheit beruht zu je einem Drittel auf technischen, organisatorischen und menschlichen Faktoren. Neben technischen Sicherheitslösungen und motivierten Mitarbeitenden muss auch die Geschäftleitung ihren Beitrag zu einem wirkungsvollen Grundschutz leisten.

Regel 2: Sichern Sie Ihre Daten regelmässig mit Backups
Datenverluste entstehen auf verschiedene Arten: Daten werden versehentlich überschrieben, Informationen auf einer Harddisk werden durch einen Defekt unleserlich oder ein Brand beziehungsweise ein Wasserschaden zerstört Ihre Daten. Solche Verluste können Sie mit regelmässigen Datensicherungen (Backups) vermeiden.

Regel 3: Halten Sie Ihr Antivirus-Programm aktuell
Schädliche Programme, wie zum Beispiel Viren und Würmer, können Ihre IT-Infrastruktur lahm legen und damit die wirtschaftliche Existenz Ihres Unternehmens gefährden.

Regel 4: Schützen Sie den Internetzugang mit einer Firewall
Gibt es in Ihrem Betrieb Brandschutztüren? Ja? Dann achten Sie bestimmt darauf, dass diese Türen auch stets geschlossen werden. In der Welt des Internets und des elektronischen Datenaustauschs erfüllt die Firewall diese Sicherheitsaufgabe.

Regel 5: Aktualisieren Sie Ihre Software regelmässig
Kontrollieren Sie bei Ihrem Auto regelmässig Ölstand und Reifendruck? Hoffentlich. So wie Sie Ihr Auto regelmässig warten, müssen auch Computerprogramme in einem Unternehmen gepflegt und auf den neuesten Stand gebracht werden.

Regel 6: Verwenden Sie starke Passwörter
Wer den Benutzernamen und das Passwort eines Anwenders kennt, kann sich an einem System anmelden und übernimmt damit die (Computer-)Identität des entsprechenden Anwenders mit allen Zugriffsberechtigungen. Durch Passwortdiebstahl können somit Unbefugte ohne grossen Aufwand an vertrauliche Geschäftsinformationen gelangen.

Regel 7: Schützen Sie Ihre mobilen Geräte
Mobiltelefone, Handheld-Computer und Notebooks mit Wireless-LAN sind ausgesprochen praktisch und vielseitig. Falsch eingesetzt, stellen diese Geräte aber ein Sicherheitsrisiko dar. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Vorkehrungen treffen.

Regel 8: Machen Sie Ihre Benutzerrichtlinien bekannt
Ohne verbindliche und verständliche IT-Benutzerrichtlinien können die Mitarbeitenden nicht wissen, welche Handlungen erlaubt und welche verboten sind. Regeln werden nur ernst genommen, wenn sich auch Vorgesetzte daran halten. Handeln Sie in allen Sicherheitsaspekten als Vorbild.

Regel 9: Schützen Sie die Umgebung Ihrer IT-Infrastruktur
Wissen Sie, wer in Ihrem Unternehmen tagsüber ein- und ausgeht? Einige wenige Vorkehrungen verhindern bereits, dass Unbefugte an wichtige Geschäftsinformationen gelangen. Gelebte, sichtbare Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten. Was nützt die beste Firewall, wenn sich Fremde in die Büroräume einschleichen können?

Regel 10: Ordnen Sie Ihre Dokumente und Datenträger
Hat Ordnung etwas mit Sicherheit zu tun? Mehr als man auf den ersten Blick vielleicht meinen möchte. Daten und Dokumente gehen auf einem ordentlichen Arbeitsplatz weniger verloren, als wenn die Arbeitsfläche mit Papieren, Handzetteln und Mäppchen übersät ist.