Neue Herausforderungen im Bereich der Informationssicherheit

Die Unternehmenssicherheit stellt sich neuen Herausforderungen, welche durch die stetige Globalisierung, Vernetzung und Komplexität verstärkt wird. Die dynamischen Veränderungen in Wirtschaft und Technik schaffen neue Gefahren und Risiken, welche sich, kombiniert mit anderen begleitenden Ereignissen wie Wirtschaftsspionage zu einer oft stark unterschätzten Risikoeinschätzung entwickeln können.

Wolfgang Sidler

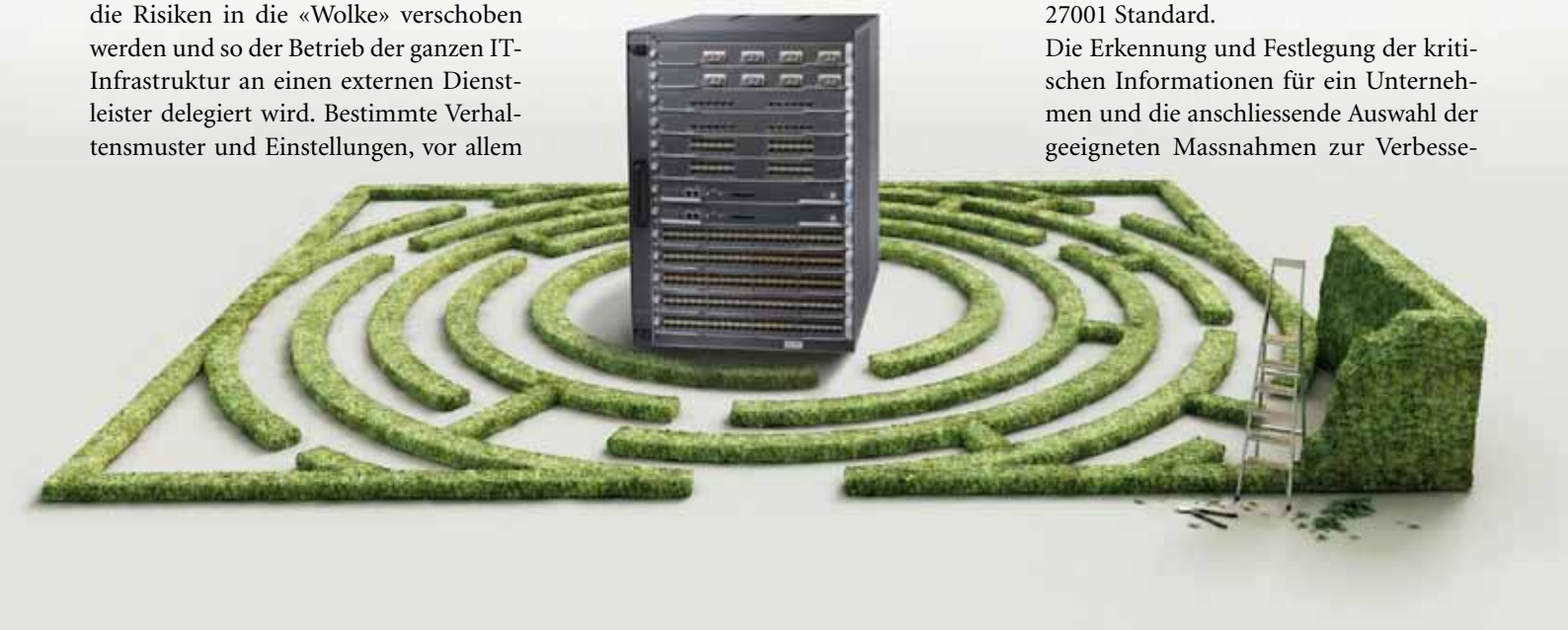
Die Chancen, die sich aus der Nutzung der Informations- und Kommunikationstechnologie ergeben, stehen aufgrund wachsender Abhängigkeit von der Technologie jedoch auch einer Vielzahl von Risiken gegenüber. Die eigentliche Herausforderung besteht darin, die unternehmensspezifischen Risiken zu identifizieren, zu bewerten, entsprechende Massnahmen einzuleiten und die Restrisiken zu kennen und zu akzeptieren. Nachrichtendienste und organisierte Kriminalität führen heute hoch professionelle IT-Angriffe durch, bei denen Informationen und IT-Strukturen von Unternehmen und auch von Privatbenutzern im Mittelpunkt des Interesses stehen. So überrascht es nicht, dass der Informationssicherheit eine immer grössere Bedeutung auf wirtschaftlicher, gesellschaftlicher, politischer und rechtlicher Ebene zukommt.

Sind bereits die meisten Unternehmer vom Virus «Cloud Computing» befallen? Mir scheint, dass genau mit diesem Hype die Risiken in die «Wolke» verschoben werden und so der Betrieb der ganzen IT-Infrastruktur an einen externen Dienstleister delegiert wird. Bestimmte Verhaltensmuster und Einstellungen, vor allem des Managements, führen zu einer erhöhten Risikobereitschaft. Jedoch unterlaufen auch System-Administratoren Fehler und viele Mitarbeitende arbeiten unvorsichtig, weil sie nicht genügend über die Risiken informiert und geschult worden sind. Das IT-Unternehmen Retarus hat im Mai 2010 Folgendes errechnet: Die Schweizer Unternehmen geben im Monat durchschnittlich CHF 4.60 pro Mitarbeiter für Klopapier aus. Nur CHF 2.70 kostet hingegen eine minimale E-Mail-Sicherheit. Vielen Firmen ist ihre Sicherheit aber nicht einmal so viel wert. Gemäss einer ETH-Umfrage geben 62 % der Betriebe nicht mehr als CHF 5000.– pro Jahr für die gesamte IT-Sicherheit aus.

Es zeigt sich, dass gewisse Unternehmen ein grösseres Risiko eines Vorfalls betreffend Informationssicherheit haben als andere. Die Grösse der Unternehmen und die Nutzung des Internets, um Geschäfte abzuwickeln, spielen dabei eine wichtige Rolle. Neben der Grösse des Unternehmens und ihrer Geschäftstätigkeit können auch andere Faktoren, wie die Art der Internetanbindung, der Grad der technischen Innovation, die Bekanntheit der Firma und die Sensibilisierung der Mitarbeitenden im Bereich der Sicherheit das Risiko eines Vorfalls beeinflussen. Eine Frage bleibt jedoch noch unbeantwortet: Viele Angriffe bleiben unentdeckt und können so in keiner Statistik oder Umfrage erfasst werden. Gerade bei gezielten Angriffen kommt es aber häufig vor, dass diese lange unentdeckt bleiben oder gar nie entdeckt werden.

Daher darf das Thema Informationssicherheit nicht ignoriert werdem. Ein Informationssicherheits-Managementsystem (ISMS) hilft, die Vielfalt der Herausforderungen systematisch in den Griff zu bekommen. Das systematische und koordinierte Planen, Steuern und Kontrollieren aller auf die Informationssicherheitsziele ausgerichteten Aufgaben bezeichnet man als ISMS und richtet sich nach dem ISO 27001 Standard.

Die Erkennung und Festlegung der kritischen Informationen für ein Unternehmen und die anschliessende Auswahl der geeigneten Massnahmen zur Verbesse-



Zehn goldene Sicherheitsregeln

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 Geschäftsleitung 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 oder 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 lahmlegen und damit die wirtschaftliche Existenz Ihres Unternehmens gefährden.

Regel 4: Schützen Sie Ihren 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. Verhindern Sie also, dass in Ihrem Betrieb der Identitätsdiebstahl möglich ist.

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 Ihre 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.

rung der Informationssicherheit sind Führungsaufgaben, die sich nur eingeschränkt delegieren lassen. Damit die Informationssicherheit erfolgreich umgesetzt werden kann, ist die volle Unterstützung des Managements unerlässlich. Die Verantwortung für die Informationssicherheit trägt das Management, das die notwendigen Massnahmen initiieren und deren Umsetzung kontrollieren muss. Achten Sie darauf, dass technische Massnahmen zur Verbesserung der IT-Sicherheit immer mit organisatorischen Massnahmen kombiniert werden müssen.

Dabei gelten die folgenden zehn Management-Grundregeln:

- Die Verantwortung für die Informationssicherheit liegt beim Management und kann nicht vollumfänglich delegiert 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 im Unternehmen integriert werden, bei denen Informationen verarbeitet und genutzt werden.
- Der Informationssicherheits-Prozess muss vom Management überwacht werden.
- Für den IT-Betrieb und die Informationssicherheit müssen ausreichende Ressourcen bereitgestellt werden.
- Es müssen organisatorische 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 nicht behindern und muss von allen als Notwendigkeit verstanden werden (Akzeptanz).
- Die IT-Sicherheitspolitik(-Strategie) muss regelmässig überprüft werden. ■

SwissSecurityDays

Am 9. März 2011 findet der Swiss SecurityDay, der nationale Tag der Computersicherheit, statt. Die jährlich abgehaltene Informationskampagne, die vom Verein InfoSurance organisiert und von Unternehmen aus der Privatwirtschaft, Banken, Versicherungen, Business- und Hochschulen, öffentlichen Organisationen, des Informatikstrategieorgans Bund ISB und der Schweizerischen Kriminalprävention getragen wird, macht an diesem Tag die Schweizer Bevölkerung auf das Thema Informationssicherheit aufmerksam und vermittelt grundlegende Schutzmassnahmen zur Vorbeugung gegen die Gefahren im Internet. Dazu werden unterschiedliche Informationskampagnen durchgeführt, die von den «5 Schritten für Ihre Computersicherheit» über verschiedene Sicherheitshinweise, Tipps & Tricks auf Intranet- und Firmen-Websites, Flyer-Aktionen für Kunden, Mitarbeiterschulungen, Online-Informationen für E-Banking-Nutzer, E-Mail- und Newslettermailings bis hin zum traditionellen Informationsstand für die Parlamentarier/-innen im Bundeshaus in Bern reichen. Im Fokus stehen dabei Themen wie Chancen und Risiken im Internet, mögliche Folgen von Datenmissbrauch, sicheres Onlinebanking, starke Passwörter und die Informationssicherheit für KMU.