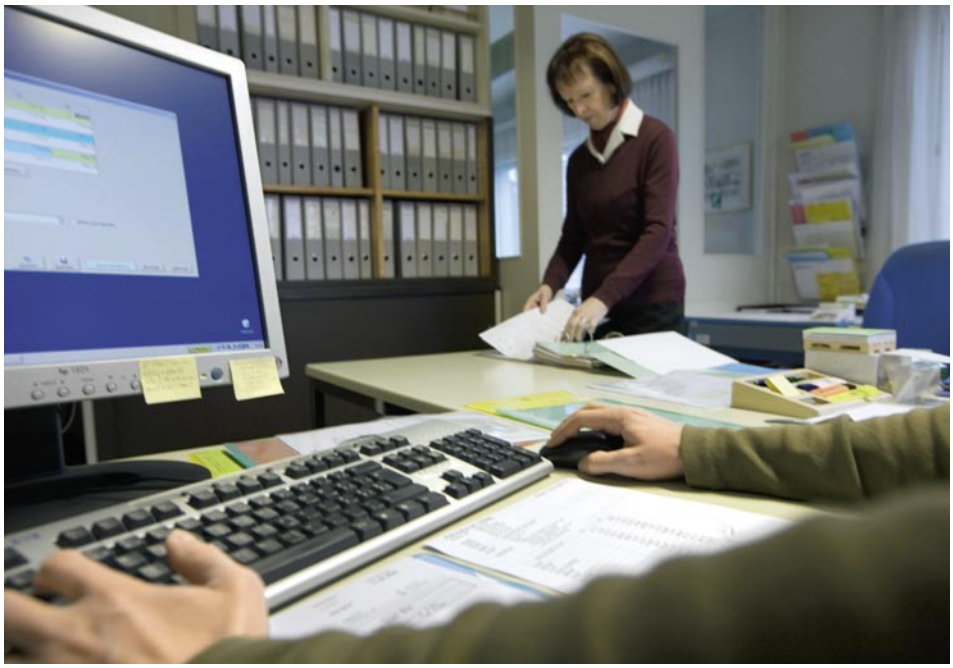
Das 10-Punkte-Programm für die Informationssicherheit bei KMU

Mit zunehmender Automatisierung und Vernetzung der Geschäftsprozesse wird Informationssicherheit auch für die kleinen und mittleren Unternehmen (KMU) ein immer wichtigeres Thema. Wie ein angemessener IT-Grundschutz ohne hohen Zeit- und Kostenaufwand zu erreichen ist, zeigt der Verein InfoSurance mit seinem einfach umsetzbaren 10-Punkte-Programm für KMU. Mit diesem Programm wird ein KMU in die Lage versetzt, notwendige Massnahmen zur Verbesserung der Informationssicherheit zu erkennen und in eigener Regie oder in Zusammenarbeit mit dem IT-Support umzusetzen.



Das 10-Punkte-Programm kann mit geringem Aufwand und selbstständig durch die KMU umgesetzt werden. Bei der Zusammenstellung des Pakets wurde besonderen Wert darauf gelegt, den speziellen Bedürfnissen und Möglichkeiten eines KMU Rechnung zu tragen. Bild: Keystone

Viren und Würmer legen ganze Informatiksysteme lahm; Unbefugte verschaffen sich Einblick in wertvolle, geheime Geschäfts- und Produktinformationen; unersetzliche Betriebsdaten gehen wegen mangelhafter Backups unwiderruflich verloren – dies sind Bedrohungen, welche den betroffenen Betrieb nicht nur viel Zeit und Geld kosten, sondern ihn im Extremfall in seiner Existenz gefährden. Während grosse Unternehmen heute den strategischen Wert ihrer Informationen kennen und einen entsprechenden Aufwand zu deren Schutz betreiben, herrscht bei den KMU – dem Rückgrat der schweizerischen Volkswirtschaft – zum Thema Informationssicherheit noch grosser Aufklärungs- und Handlungsbedarf.

Prof. Carlos Rieder
Dipl. El.-Ing. FH, Leiter Informationssicherheit Hochschule Luzern – Wirtschaft, Inhaber isec ag Luzern, Präsident Verein InfoSurance

Einfach umsetzbarer Minimalstandard

Hier will der Verein InfoSurance – eine gemeinsame Institution von Wirtschaft und Staat – in Zusammenarbeit mit Verbänden und anderen KMU-nahen Institutionen und Unternehmen einen Beitrag leisten. Eine Gruppe von Fachleuten rund um InfoSurance hat ein IT-Grundschutz-Set entwickelt: das 10-Punkte-Programm für KMU (siehe *Kasten 1*). Die darin enthaltenen Regeln verstehen sich als Minimalstandard und sind in jedem Unternehmen anwendbar. Ihre Einhaltung muss von der Geschäftsleitung im Rahmen ihrer Sorgfaltspflicht periodisch überprüft werden.

Das Programm kann mit geringem Aufwand und selbstständig durch die KMU umgesetzt werden. Bei der Zusammenstellung des Pakets wurde besonderen Wert darauf gelegt, den speziellen Bedürfnissen und Möglichkeiten eines KMU Rechnung zu tragen. Es liegt auf der Hand, dass hier nicht dieselben personellen und finanziellen Ressourcen zur Gewährleistung des Informationsschutzes zur Verfügung stehen wie etwa bei einer Grossbank. Im Gegensatz zur gängigen Meinung ist die Etablierung eines elementaren Sicherheitsstandards im Betrieb aber nicht zwangsläufig mit hohen Kosten verbunden. Mindestens ebenso wichtig wie technische Vorkehrungen sind organisatorische Massnahmen – vor allem aber der Wille zu deren konsequenter Umsetzung durch die gesamte Belegschaft.

Informationssicherheit ist kein Selbstzweck

Informationssicherheit ist kein Selbstzweck, sondern dient letztlich dem Schutz der Investitionen und dem Erfolg eines Unternehmens. Nicht alle KMU haben jedoch die gleichen Bedürfnisse. Während die einen mit sehr vertraulichen Informationen und sensiblen Personendaten zu tun haben (z.B. Treuhänder, Juristen, Ärzte), sind andere auf eine hohe Verfügbarkeit ihrer Informatikmittel angewiesen (z.B. produzierende Unternehmen, Grafiker, Druckereien). Interessanterweise geht eine grosse Zahl von KMU davon aus, dass ihre Unternehmen kein lohnendes Ziel für Hacker seien. Dies ist falsch, denn ungeschützte Systeme sind ein gefundenes Fressen und werden so manipuliert, dass sie zu Elementen eines riesigen «Schwarmes» von Systemen werden, die gemeinsam einen grossen, verteilten Angriff durchführen. In verschiedenen Fällen wurden die Verantwortlichen der Unternehmung wegen Verletzung ihrer Sorgfaltspflicht zur Rechenschaft gezogen.

Die zehn Punkte des Programms

Verantwortlichkeiten

Legen Sie die Verantwortlichkeiten rund um die Informationssicherheit fest. Wer ist der zentrale Ansprechpartner? Wer führt die Datensicherung durch? Die Informationssicherheit muss von allen getragen werden. Alle Mitarbeitenden müssen ihren Beitrag leisten, etwa indem Verschwiegenheit gegenüber Aussenstehenden gewahrt wird. Die oberste Verantwortung trägt jedoch immer die Geschäftsleitung. Um ihrer Sorgfaltspflicht gerecht zu werden, muss sie sich mit dem Thema auseinandersetzen. Eine Delegation an die IT ist weder möglich noch sinnvoll.

Datensicherung

Eine vollständige, aktuelle Datensicherung ist das A und O der Informationssicherheit. Alle relevanten Daten müssen täglich gesichert werden. Die Sicherung soll in Generationen erfolgen (z.B. Montag Band 1, Dienstag Band 2 usw.). Auch Wochen- und Monatsbänder sind sinnvoll. Eine regelmässige Kontrolle, ob die gesicherten Daten auch tatsächlich wieder zurückgelesen werden können, ist ebenfalls zwingend notwendig. Backup-Medien müssen an einem sicheren Ort aufbewahrt werden, mitunter ausserhalb der Unternehmung.

Virenschutz

Ein Viren- oder Malware-Schutz ist heute zum Glück beinahe Standard. Wichtig ist aber auch, dass dieser regelmässig mit den neusten Virensignaturen versorgt wird, sonst nimmt sein Schutzwert schnell ab und er wird wertlos. Somit müssen die Aktualisierungsabonnemente regelmässig erneuert werden, und das Virenprogramm muss seine Signaturlisten täglich aktualisieren können. Auch muss regelmässig geprüft werden, ob der Virenschutz tatsächlich noch gestartet ist und läuft.

Firewall

Dass das Internet neben grossen Vorteilen auch neue Möglichkeiten für Missbrauch eröffnet, ist nichts Neues. Die Firewall überwacht die Verbindung zwischen Computer und Internet und verhindert unzulässige Zugriffe. Es ist sehr wichtig, nicht nur die Verbindungen vom Internet nach innen zu überwachen, sondern auch die umgekehrte Richtung. Allenfalls eingeschleuste Trojaner (Schadenssoftware) versuchen, Daten aus dem Netzwerk der Unternehmung nach aussen zu übermitteln. Auch eine Firewall braucht Wartung und muss regelmässig kontrolliert werden, um Angriffsversuche zu erkennen.

Software-Updates

Software ist sehr komplex. Bei der Entwicklung schleichen sich Fehler ein, welche von potenziellen Angreifern missbraucht werden. Die Hersteller bieten für sicherheitsrelevante Fehler Korrekturen an, so genannte Patches. Diese müssen schnellstmöglich installiert werden, um potenzielle Schwachstellen zu beseitigen, bevor sie ausgenutzt werden können. Noch vor Jahren vergingen Wochen, ja Monate, bevor eine erkannte Schwachstelle ausgenutzt wurde; heute sind

Kasten 1

Das 10-Punkte-Programm

1. Zuweisung der Verantwortlichkeiten
2. Datensicherung
3. Schutz vor Computerviren
4. Sichere Verbindung ins Internet
5. Software-Aktualisierung; Patches
6. Umgang mit Passwörtern
7. Schutz mobiler Geräte
8. Benutzerrichtlinien
9. Physischer Schutz der IT
10. Ordnung

Kasten 2

Verein InfoSurance

Der Verein InfoSurance ist eine gemeinsame Institution von Wirtschaft und Staat für einen sicheren Informations- und Kommunikationsplatz Schweiz mit dem Schwergewicht KMU und Heimanwender. Sie will organisatorische und infrastrukturseitige Voraussetzungen schaffen, damit den Risiken der zunehmenden Abhängigkeit von Informationstechnologien wirkungsvoll und effizient begegnet werden kann.

Nähere Informationen über den Verein InfoSurance finden Sie auf der Website *www.infosurance.ch*.

Bild: Rieder

Massnahmen zur Sicherstellung der Informationssicherheit braucht es auch wegen möglicher äusserer Gefahren. Im Bild: Hochwasser in der Luzerner Altstadt, August 2005.

es oft nur noch Tage. Somit ist eine unverzügliche Installation der Patches zwingend nötig.

Passwörter

Ein ungeeigneter Umgang mit Passwörtern führt zu Identitätsmissbrauch. Nach wie vor werden Passwörter vom arbeitenden Personal als störendes Übel erachtet. Das Abschliessen des Zuganges zur Firma mit dem Schlüssel ist eine Selbstverständlichkeit; das Verwenden eines Bildschirmschoners mit Passwort wird hingegen nur mit grossem Missfallen akzeptiert. Das Passwort schützt die digitale Identität und ist somit sehr vertraulich zu handhaben. Weiter muss auch die Qualität der Passwörter stimmen: mindestens 8 Stellen, grosse und kleine Buchstaben, Zahlen und Sonderzeichen, keine Verwendung von Namen, Ortschaften usw. Wenn das Passwort aufgeschrieben werden muss, dann bitte persönlich verwahren, nicht als Post-it am Bildschirm oder unter der Tastatur!

Mobile Geräte

Moderne mobile Geräte – wie Handys und PDAs – sind kleine, leistungsfähige Computer mit gewaltigen Speicherkapazitäten. Dies gilt untern anderem auch für iPods, MP3-Player, Digitalkameras und Memory-Sticks. Problemlos lassen sich damit die Daten ganzer Archive innert Minuten kopieren. Falls dies nicht im Sinne der Unternehmung ist, müssen diese Möglichkeiten auf technischer Ebene und/oder mittels Weisungen unterbunden werden. Auf jeden Fall müssen die mobilen Geräte so geschützt werden, dass die darauf gespeicherten Daten nicht von unberechtigten Dritten eingesehen werden können.

Benutzerrichtlinien

Die Anwendung der Informatikmittel muss geregelt sein. Was ist zulässig und was nicht? Angepasste, umsetzbare Benutzerweisungen legen fest, wie die zur Verfügung gestellten Computer eingesetzt werden dürfen. Dürfen eigene Programme installiert werden? Darf der Virenschutz ausgeschaltet werden, damit die Anwendungen schneller laufen? Dürfen Daten auf der lokalen Festplatte abgelegt werden? Diese und weitere Fragen müssen geklärt sein. Benutzerrichtlinien dürfen nicht zu einem Papiertiger verkommen. Die Umsetzung durch alle Mitarbeitenden ist durchzusetzen.

Zutritt zur Infrastruktur

Der Zutritt zur Unternehmung muss im Rahmen des Möglichen und Sinnvollen geregelt sein. Die Server und die Netzwerkinfrastruktur gehören eingeschlossen und für Dritte nicht zugänglich. Auch muss der Zutritt zu den Büroräumen oder zur Produktion kontrolliert erfolgen. Die ganzen Massnahmen zum Schutz der Informationen in den Computern sind wenig sinnvoll, wenn die wertvolle Information einfach in verwaisten Büros beschafft werden kann.

Ordnung

Auch im Computer müssen die Dokumente nachvollziehbar abgelegt werden. Eine sinnvolle, funktionelle Ablagestruktur spart regelmässigen Suchaufwand. Dass zumindest abteilungsintern ein einheitliches System verwendet wird, ist von grosser Bedeutung. Arbeitsplätze mit vertraulichen Daten sind beim Verlassen immer aufzuräumen; die Clear-Desk-Politik ist anzuwenden. Bei der Entsorgung von Daten muss auf eine zuverlässige Vernichtung geachtet werden. Papier gehört in den Schredder; ausgediente Computer müssen mit einer speziellen Software gelöscht werden (Wiping), oder die Datenträger sind endgültig zu zerstören. ▮

Kasten 3

Broschüre und IT-Sicherheitshandbuch für KMU

Das 10-Punkte-Programm kann als Broschüre von der Website der InfoSurance *www.infosurance.ch* heruntergeladen werden. Bestellungen der gedruckten Broschüre oder Fragen im Zusammenhang mit Informationssicherheit in KMU richten Sie bitte an *info@infosurance.ch*.

Für weiterführende Informationen empfehlen wir das *IT-Sicherheitshandbuch für die Praxis*. Grundsätzliches wird erklärt und mit vielen Praxisbeispielen untermauert. Die beiliegenden Checklisten und Vorlagen unterstützen die Umsetzung. Das Handbuch kann auf *www.sihb.ch* bestellt werden.