SICHERHEIT bringt GELD!

HERBERT FIDESSER

Geschäftsführender Obmann der ÖSIT Tea.GenmbH. die sich mit Schulungen und Beratungen im Bereich der IT-Sicherheit beschäftigt.
fidesser@ösit.at

►IT-Security für Freiberufler und Kleinunternehmen

In der Geschäftswelt sehen wir eine wachsende Abhängigkeit vom Funktionieren der Informationstechnik (IT), immer mehr Geschäftsprozesse werden auf IT-Systeme verlagert oder mit ihnen verzahnt. IT-Sicherheit ist daher integraler Bestandteil der originären Aufgabe aller Unternehmen.
Das Erreichen eines angemessenen Sicherheitsniveaus wird nur durch einen IT-Sicherheitsprozess, der auf einer planmäßig anzuwendenden, begründeten Vorgehensweise beruht, gewährleistet.
Das Erstellen der entsprechenden, unternehmensbezogenen IT-Sicherheitsrichtlinie ist ein extrem zeit- und kostenaufwendiger Prozess. Die notwendigen Mittel stellen derzeit nur größere Unternehmen bereit; Klein-unternehmer und Freiberufler verzichten (z. T. auch aus Mangel an Information) darauf und nehmen damit hohe Risiken in Kauf.
Eine grobe Kostenschätzung zeigt, dass die Entwicklung einer funktionierenden und überprüfbaren Sicher-heitsrichtlinie für KUs mit Kosten von ca. € 25.000,- (Eigen- und Fremdleistung) verbunden ist. Stichproben-Befragungen zeigen aber, dass (nach Erkennen des Schutzbedarfs) die Geschäftsleitungen zu einer Investition von maximal 10% dieses Betrages bereit sind.

► Der Grundschutzansatz

Die Firma ÖSIT, ein Startup von engagierten Unternehmensberatern, Security-Spezialisten, Netzwerkadmini-stratoren, macht mit dem genannten Grundschutzansatz eine angemessene IT-Sicherheit auch für Kleinun-ternehmen leistbar. Information, Schulungsmaßnahmen und einfach zu handhabende Softwaretools sind die dafür entwickelten Hilfsmittel. Die Entscheidung darüber, was „angemessen" ist, verbleibt dabei immer beim Unternehmen:
Bei der Definition des geplanten Sicherheitsniveaus bedient man sich im Allgemeinen des Österreichischen IT-Sicherheitshandbuches des Stabsstelle IKT-Strategie des Bundes, das im Wesentlichen den Vorgaben des IT-Grundschutzhandbuches[1] des BSI[2] folgt.
Hauptziel des Grundschutzansatzes ist es, den Zeit- und Kostenaufwand für die Erstellung eines IT-Sicherheitskonzeptes angemessen zu begrenzen. Erreicht wird das dadurch, dass von einer pauschalisierten Gefährdungslage ausgegangen, diese auf die unternehmensspezifischen Notwendigkeiten angepasst und damit auf eine detaillierte Risikoanalyse verzichtet wird.
Die Vorteile dieser Vorgehensweise sind der stark reduzierte Aufwand für die Risikoanalyse und ein rasch zu erreichendes, relativ hohes Niveau an Sicherheit gegen die häufigsten Bedrohungen. Zudem sind Grund-schutzmaßnahmen meist stark verbreitet und damit relativ kostengünstig und schnell zu implementieren.

► So bleiben die Investitionen bescheiden

Die ÖSIT hat eine IT-Security-Datenbank entwickelt. Sie ist das wichtigste Tool zur raschen und kostengün-stigen Erstellung von IT-Sicherheitsrichtlinien und enthält neben den Elementen des Grundschutzhandbuchs auch die nötigen Ein- und Ausgabeobjekte.

1. Eine ÖSIT-Vorauswahl schließt die für bestimmte Branche oder Gruppe von Freiberuflern irrelevanten Gefährdungen und Maßnahmen aus der Betrachtung aus. Die verbleibenden Elemente bilden die Grund-lage für eine Muster- IT-Sicherheitsrichtlinie.
2. Darstellung des IT-Verbundes: Für alle IT-Systeme (PCs, Netzelemente, Telefonanlagen usw.) werden Systemübersichten („PC-Pässe") erstellt. Neben den technischen Daten enthalten diese auch das jeweils angestrebte Sicherheitsniveau für die Kategorien Vertraulichkeit, Authentizität, Integrität und Verfügbar-keit.
3. Mittels der von der ÖSIT entwickelten Online-Tools beantwortet die Unternehmensleitung im Zuge ei-nes ÖSIT-Workshops die Fragen zu den relevanten Maßnahmen. Die Antworten haben Rückwirkungen auf die Feindefinition der unternehmensspezifischen IT-Sicherheitsrichtlinie. Typische Fragen sind z.B. „Wird regelmäßig überprüft, ob die Fenster und Türen nach Verlassen der Räume verschlossen sind?" oder „Ist die Einschränkung der Benutzerumgebung aus betrieblicher Sicht notwendig?" oder „Werden periodisch Kontrollen durchgeführt, um die Integrität der installierten Programme zu überprüfen?"
4. Schließlich ergeben sich daraus die zu evaluierenden Maßnahmen. Jede einzelne Maßnahme muss für jedes betroffene IT-System evaluiert werden. Der Befund kann auf „entbehrlich", „bereits umgesetzt", „teilweise umgesetzt" oder „nicht umgesetzt" lauten. Weiters sind auch ein Umsetzungstermin, die Verantwortlichkeit und bei Bedarf eine Kostenschätzung festzulegen. Alle Ergebnisse werden im Online Tool, das dem Unternehmen jederzeit zur Verfügung steht, gespeichert. So können der Stand der Umsetzung und notwendige weitere Maßnahmen jederzeit überprüft werden.

5. Da die Risikoanalyse ein regelmäßig wiederkehrender Prozess ist, sind die Schritte 2 bis 4 mit jeder Anschaffung eines IT-Systems oder einer Anwendung zu berücksichtigen sowie im Anlassfall bzw. in periodischen Abständen zu wiederholen.

▶Erstellung der IT-Sicherheitsrichtlinie

Die faktische Erstellung einer IT-Sicherheitsrichtlinie erfolgt in mehreren Schritten:

1. Sensibilisierung des Managements (in *v*SIT-Informationsveranstaltungen, via Internet usw.)
2. Erstellung der Systemübersichten/PC-Pässe durch Unternehmensleitung und IT-Verantwortliche (ge-meinsam).
3. *v*SIT-Security Training und -Workshop: Teilnehmer: Management und IT-Verantwortliche (in vielen Fällen identisch) mehrerer Unternehmen (Kleingruppe). Dabei wird eine „Handlungsanleitung" zur Erstellung einer IT-Sicherheitsrichtlinie erarbeitet. Es werden die notwendigen Fragen durchgearbeitet und eine erste Version der erstellt.
4. Im eigenen Unternehmen wird gemeinsam mit den betroffenen Mitarbeitern die Notwendigkeit jeder einzelnen Maßnahme nochmals überprüft und die endgültige IT-Sicherheitsrichtlinie veröffentlicht und in Kraft gesetzt.

Auf Wunsch ist auch eine Zertifizierung nach ISO 27001-Zertifikate möglich.

▶Was haben Sie davon?

Der wichtigste Kundennutzen ist wohl der zuverlässige Schutz von Informationen, Dokumenten und Daten vor Verlust, Diebstahl und Verfälschung, wobei Aufwand und Grad der Risikominderung gegeneinander abgewogen werden. Ein mit *v*SIT-Unterstützung erstelltes Sicherheitskonzept zeichnet sich weiter aus durch einen vollständigen Grundschutz, eine kurze, die Personalressourcen schonende Erarbeitungszeit (Zeitfaktor), den äußerst günstigen Preis und Klarheit im Aufbau und somit hohe Akzeptanz nach innen und außen.
Klare, verpflichtende Festlegung des unternehmensspezifischen Sicherheitsniveaus für

- Vertraulichkeit (Information nur an zuständigen Adressatenkreis),
- Authentizität (Nutzer ist tatsächlich die Person, für die er sich ausgibt),
- Integrität (Vollständigkeit, Unversehrtheit und Korrektheit der Daten) und
- Verfügbarkeit (Definierte Dienste oder Systeme sind zu vereinbarten Zeiten nutzbar).

Anmerkungen:

[1] Das Grundschutzhandbuch besteht aus ca. 2.500 Seiten. In 64 Bausteinen werden 379 Gefährdungen und 921 Maßnahmen aufgelistet.. Schon aus diesen Zahlen wird klar, dass KMUs weder personell noch finanziell in der Lage sind, ein entsprechendes Sicherheitskonzept allein zu erstellen.

[2] Bundesamt für Sicherheit in der Informationstechnik (D)

Meldung des grenzüberschreitenden Dienstleistungsverkehrs

Grenzüberschreitende Dienstleistungen sind ab 2006 bei der Statistik Austria meldepflichtig. Diese Meldepflicht wurde in der Meldeverordnung der Österreichischen Nationalbank – Amtsblatt der Wiener Zeitung Nr. 149 vom 3. 8. 2005 - festgelegt.

Dazu einige Erläuterungen:

- **Meldepflichtig** sind alle natürlichen oder juristischen Personen sowie die Personengesellschaften des Handelsrecht und die Erwerbsgesellschaften, die ihren Sitz bzw. Wohnsitz im Inland haben, bestimmte Wirtschaftstätigkeiten betreiben (fast alle Tätigkeiten sind betroffen) und
- grenzüberschreitende Dienstleistungen **für das Ausland** erbringen oder
- grenzüberschreitende Dienstleistungen **aus dem Ausland** beziehen, und
- **bestimmte Schwellenwerte übersteigen**.

Schwellenwerte

Die Schwellenwerte für Dienstleistungsexporte reichen branchenbezogen von der Erlössumme von 50.000,– bis zu 200.000,– im Vorjahr. Auch bei den Dienstleistungs-importen betragen die Schwellenwerte von 50.000,– bis 200.000,– im Vorjahr.
Wenn Ihr Dienstleistungsexport bzw. -import den Jahresbetrag von jeweils 50.000,– nicht übersteigt, sind Sie in jedem Falle von dieser Meldepflicht befreit.

Meldefristen

Die Meldung muss quartalsweise bis zum 15. des Folgemonats, also **erstmals für das 1. Quartal 2006** und zusätzlich jährlich bis 15.2. des folgenden Jahres erfolgen (Formular L2/ST.AT). Die Frist ist um einen Monat verlängerbar. Auch die elektronische Meldung ist zulässig. Von Vorteil ist es, wenn Ihr FiBu-Programm diese Meldung unterstützen kann, so z. B. durch Hinterlegung bestimmter Codes bei den betreffenden Erlös- bzw. Aufwandskonten mit entsprechender Gliederung nach den „Partnerländern".

Auskünfte

Von der Homepage der Österreichischen Nationalbank können Sie sich die „Meldeverordnung ZABIL 1/2005 der ÖNB betreffend die statistische Erfassung des grenzüberschreitenden Dienstleistungsverkehrs" herunterladen (16 Seiten).

Bei Fragen über die elektronische Übermittlung: www.netquest.at