Mehr Informationssicherheit für KMU (Teil 2)

Text **André Schmid***
Bilder **red.**

Der erste Teil der zweiteiligen Folge über die Verwendung von EDV in kleinen und mittleren Unternehmen (vgl. applica 20/2005, S. 10) behandelte die ersten fünf Schritte auf dem Weg zu einem sicheren Einsatz der modernen Informationstechnologie. Der zweite Teil umfasst nun die zweiten fünf Schritte sowie ein Glossar.

Schritt 6: Mobile Geräte vor unbefugtem Zugriff und Manipulation schützen

Zugegeben, ausgesprochen praktisch, vielseitig und schick sind sie ja, die Mobiltelefone, die kleinen Handheld-Computer und die Notebooks mit Wireless LAN (drahtlosem Netzwerkanschluss). Aus dem Geschäftsalltag sind sie auf jeden Fall nicht mehr wegzudenken. Doch falsch eingesetzt, bedeuten sie für jeden Betrieb ein immenses Sicherheitsrisiko, besonders wenn heikle Geschäftsdaten auf ihnen gespeichert sind. Wer aus geschäftlichen Gründen gezwungen ist, sensible Daten auf mobilen Geräten zu speichern, muss spezielle Sicherheitsvorkehrungen treffen:

- Sorgen Sie dafür, dass auf mobilen Geräten nur diejenigen Daten enthalten sind, die tatsächlich benötigt werden.
- Sämtliche mobilen Geräte müssen mit einem starken Passwort geschützt werden (siehe Schritt 7). Beim Verlust des Geräts oder im Fall eines Diebstahls ist es für Unbefugte sonst ein Leichtes, an Ihre vertraulichen Geschäftsdaten zu gelangen.
- Heikle Firmendaten auf Notebooks müssen verschlüsselt gespeichert werden, damit sie bei Verlust oder Diebstahl nicht in die Hände Unbefugter geraten. Gute Verschlüsselungsprogramme sind im Handel erhältlich und können auch aus dem Internet heruntergeladen werden (z.B. PGP – Pretty Good Privacy – www.pgp.com).
- Über falsch eingesetzte Wireless-LAN-Geräte können Hacker aus Distanzen bis zu 500 m mit einfach zu bedienenden Programmen innerhalb von Minuten in Ihr Firmennetzwerk einbrechen! Besondere Vorsicht ist auch geboten, wenn Sie oder Ihre Mitarbeiter von einem externen Zugangspunkt (sog. Hot Spot) auf das Firmennetz zugreifen.
- Aktivieren Sie bei Geräten mit Bluetooth (Handy, mobile Agenda, Handheld-Computer) diese Funktion nur bei Bedarf. In der übrigen Zeit ist die Bluetooth-Funktion zu deaktivieren. Sonst laufen Sie Gefahr, dass Ihr Gerät im Umkreis von bis zu 100 m ohne Ihr Wissen auf die Anfragen von anderen Bluetooth-Geräten antwortet.
- Tauschen Sie über Bluetooth nur Daten mit Personen aus, denen Sie vertrauen.

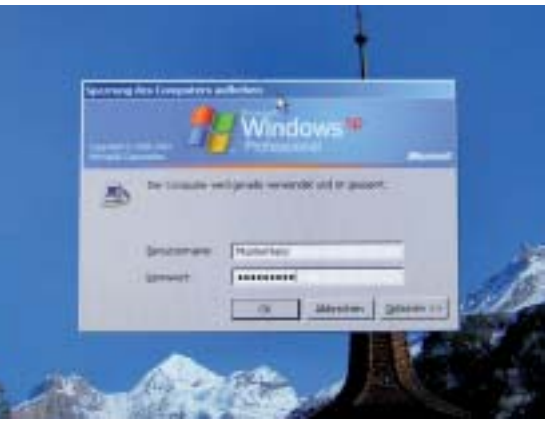
Auf mobilen Geräten sollen nur die wirklich benötigten Daten gespeichert und diese mit einem starken Passwort geschützt werden.

* Geschäftsleiter InfoSurance (Stiftung für einen sicheren Informations- und Kommunikationsplatz Schweiz), www.infosurance.ch

Sicherer Umgang mit Wireless LAN
Die folgenden sechs Massnahmen führen zu einem sicheren Umgang mit Wireless LAN inner- und ausserhalb des Unternehmens:

– Ändern Sie den vom Hersteller vorgegebenen Namen für Ihr kabelloses Netzwerk (Service Set ID – SSID). Verwenden Sie als neue Identifikation keinesfalls Ihren Firmennamen oder einen Begriff, der Rückschlüsse auf Ihre Tätigkeit erlaubt.
– Ändern Sie das Standardpasswort Ihres Zugangspunkts. Verwenden Sie ein starkes Passwort (siehe Schritt 7).
– Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung WEP (Wired Equivalent Privacy). Wählen Sie wenn möglich eine 128-Bit-Verschlüsselung. Ändern Sie den vom Hersteller standardmässig eingestellten WEP-Schlüssel. Vorsicht: Der WEP-Schlüssel kann von speziellen Hackerprogrammen innerhalb von ein bis zwei Stunden geknackt werden. Der WEP-Schlüssel sollte deshalb regelmässig gewechselt werden.
– Verwenden Sie einen MAC-Adressen-Filter, falls Ihr Produkt diese Option bietet.
– Deaktivieren Sie die ungerichtete SSID-Ausstrahlung.
– Wireless-LAN-Geräte sollten ausschliesslich in einem Virtual Private Network (VPN, abhörsichere Internetverbindung) betrieben werden. Wird eine Verbindung ins Firmennetz über einen öffentlichen Zugangspunkt hergestellt, darf dies nur über VPN erfolgen. Viele Betriebssysteme beinhalten bereits ein VPN-System. Nutzen Sie es!

Schritt 7: Passwörter und Identität vor Missbrauch schützen



Ein starkes Computerpasswort ist mindestens acht Zeichen lang und enthält Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen.

Wer Ihr Computerpasswort oder das Ihrer Mitarbeiter kennt und sich damit einloggt, besitzt Ihre Identität und verfügt über Ihre Berechtigungen. Durch Passwortdiebstahl können Unbefugte einfach an wichtigste Geschäftsinformationen gelangen. Verhindern Sie also, dass in Ihrem Betrieb der Identitätsdiebstahl möglich ist. Halten Sie Ihre Mitarbeiter dazu an, nur starke Passwörter einzusetzen, die regelmässig geändert werden. Machen Sie allen bewusst, dass sie für Handlungen verantwortlich sind, die unter ihrem Benutzernamen ausgeführt werden.

Starke Passwörter sind mindestens acht Zeichen lang und enthalten Gross- und Kleinbuchstaben, Zahlen sowie Sonderzeichen.

Passwortmerkregel einsetzen

Anstelle des Passwortes merkt man sich einen geheimen Satz, was viel einfacher ist. Dem starken Passwort V2Jfd€u6% liegt der Satz «Vor 2 Jahren fiel der Euro um 6 Prozent» zugrunde. Um dieses Passwort zu erkennen, benötigt ein Hackerprogramm rund sechzig Jahre. Weitere Beispiele: Der Fragesatz «Fahren wir in 2 × 7 Tagen zu dritt nach Paris?» ergibt das starke Passwort «Fwi2x7TzdnP?».

Wenn Sie unsicher sind, ob Ihr Passwort stark ist, können Sie unter www.datenschutz.ch mit einem ähnlichen Passwort einen Test durchführen. Ein Passwort-Check macht Spass und ist ein gutes Mittel zur Mitarbeitersensibilisierung.

Nicht vergessen:

– Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden (gehört ins Pflichtenheft des IT-Verantwortlichen).
– Der Stellvertreter des IT-Verantwortlichen muss wichtige Passwörter ebenfalls kennen. Andernfalls kann er unter Umständen seine Stellvertreterfunktion gar nicht wahrnehmen.

Verbotene Passwörter und unzulässige Handlungen mit Passwörtern

Folgende Passwörter sollten nicht verwendet werden:

– Weniger als acht Zeichen lang
– Wörter und Namen, die in Wörterbüchern oder Dictionnaires zu finden sind – sie werden von einem Hackerprogramm mit Leichtigkeit erkannt
– Namen und Geburtsdaten aus dem Familienumfeld – sie können von Kollegen oder Bekannten leicht erraten werden
– AHV- und Passnummern
– Namen und Begriffe aus dem Hobbybereich
– Zahlen- und Buchstabenfolgen, wie z.B. 1234, abcde oder asdf

Passwörter dürfen weder auf Zetteln noch im Computersystem notiert werden. Zudem sollte ein Passwort mindestens alle ein bis zwei Monate geändert werden (evt. Passwortwechsel forcieren durch IT-Verantwortlichen). Ebenso wenig darf ein Passwort an Dritte weitergegeben werden. Falls dies trotzdem einmal geschehen musste, ist das Passwort anschliessend umgehend zu wechseln.

Schritt 8: IT-Richtlinien schaffen Klarheit und Sicherheit bei Ihren Mitarbeitern

Ist bei Ihnen im Betrieb «erlaubt, was nicht stört»? Ohne verbindliche und verständliche Sicherheitsrichtlinien können Ihre Mitarbeiter nicht wissen, welche Handlungen erlaubt und welche verboten sind. Überlassen Sie die Sicherheit Ihrer Daten nicht dem Gutdünken Ihrer Mitarbeiter.

Allerdings werden Sicherheitsvorkehrungen von vielen als störend empfunden. Sensibilisieren Sie deshalb Ihre Mitarbeitenden regelmässig für die Sicherheit in Ihrem Betrieb. Sicherheitsregeln werden nur ernst genommen, wenn auch die Chefin und der Chef sie einhalten. Handeln Sie in allen Sicherheitsaspekten immer als Vorbild.

IT-Richtlinien für Mitarbeiter

Geben Sie schriftliche Sicherheits- und IT-Richtlinien heraus und lassen Sie sie von Ihren Mitarbeitern unterschreiben. In den Richtlinien wird Folgendes geregelt:

- Umgang mit Passwörtern (siehe Schritt 7)
- Verbot von Einsatz und Installation nicht genehmigter Programme
- Verbot nicht genehmigter Hardware-Komponenten
- Festlegung des Internetgebrauchs: Informationen dürfen aus dem Internet heruntergeladen werden, nicht aber Programme. Der Besuch von Chatrooms und Webseiten mit pornografischen, rassistischen und sexistischen Inhalten ist untersagt.
- Gebrauch von E-Mail
- Umgang mit Antivirus-Programm inkl. Aktualisierung (sofern dies nicht zentral vorgenommen wird)
- Umgang mit Sicherheits-Patches (sofern dies nicht zentral vorgenommen wird)
- Datensicherung und Aufbewahrungspflicht (sofern diese nicht zentral vorgenommen werden)
- Einhalten des vorgegebenen Ordnungssystems (siehe Schritt 10)
- Umgang mit Daten, die dem Datenschutzgesetz unterstehen
- Umgang mit internen, vertraulichen und geheimen Informationen und Daten
- Verhalten bei sicherheitsrelevanten Vorkommnissen, z.B. bei Viruswarnungen, Diebstählen und Verlust von Notebooks oder Passwörtern – IT-Verantwortlicher muss sofort informiert werden
- Disziplinarmassnahmen und Sanktionen für den Fall, dass gegen die internen Sicherheitsrichtlinien verstossen wird.

Veranlassen Sie eine Basisausbildung aller Mitarbeitenden, z.B. auf Grundlage dieser Broschüre. Wichtigste Lernziele:

- Bestimmen starker Passwörter (siehe auch Schritt 7)
- Sicherer Umgang mit Internet und E-Mail
- Sicherer Umgang mit dem Virenschutzprogramm
- Ablegen und Sichern von Dokumenten
- Verstehen der Sicherheits- und IT-Richtlinien

Führen Sie ein- bis zweimal pro Jahr Sicherheits- und Sensibilisierungskampagnen durch. Dies ist mit einfachen Mitteln möglich, z.B. E-Mails an alle Mitarbeiter, interne Rundschreiben, Plakate im Eingangsbereich und in der Kantine. Beiträge in der Firmenzeitung usw. leisten ebenfalls wertvolle Dienste.

Damit die Sicherheitsregeln im Berufsalltag auch richtig befolgt werden, muss man den Mitarbeitern klare Richtlinien vorschreiben.

Schritt 9: Sichtbar gelebte Sicherheit schafft Vertrauen

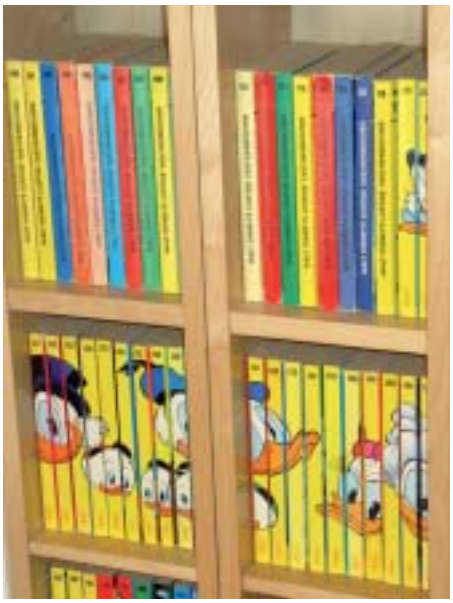
Wissen Sie, wer bei Ihnen über den Tag so alles ein und aus geht? Und können Sie für sämtliche Besucher die Hand ins Feuer legen? Einige wenige Vorkehrungen verhindern bereits, dass wichtige Geschäftsinformationen durch Unachtsamkeit an Unbefugte gelangen. Gelebte Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten.

Mit folgenden Massnahmen schaffen Sie mehr Sicherheit:

- Lassen Sie Besucher, Kunden und Bekannte nicht unbeaufsichtigt in Ihrem Betrieb umhergehen.
- Alle Drittpersonen werden am Empfang abgeholt und auch stets wieder zum Ausgang begleitet.
- Wer den Empfang nicht dauernd besetzt halten kann, lässt die Eingangstür verschlossen und bringt ein Schild «Bitte läuten!» an.
- Sorgen Sie dafür, dass Schlüssel und Badges korrekt verwaltet und die entsprechenden Listen aktuell gehalten werden. Schlüssel mit Passepartout-Funktion sind nur restriktiv zu verteilen. Die entsprechenden Berechtigungen müssen periodisch auf ihre Notwendigkeit überprüft werden.
- Mitarbeitende, die aus dem Unternehmen austreten, müssen ihre Schlüssel, Badges und Zugangsberechtigungen beim Austritt abgeben.
- Stellen Sie sicher, dass sämtliche Eingangstüren (auch hinten), Lichtschächte und Parterrefenster über einen ausreichenden Einbruchschutz verfügen. Entsprechende Informationsblätter sind bei der örtlichen Polizei erhältlich.
- Server gehören in verschlossene Räume, zu denen nur der IT-Verantwortliche und sein Stellvertreter Zutritt haben. Wo dies nicht möglich ist, wird der Server wenigstens in einen abschliessbaren Computerschrank eingebaut.
- Brennbares Material wie Papier usw. darf nicht im Serverraum gelagert werden.
- Sorgen Sie dafür, dass im Serverraum oder in unmittelbarer Nähe ein gut sichtbarer CO_2-Feuerlöscher platziert wird.
- Netzwerkdrucker gehören nicht in öffentlich zugängliche Räume, da Unbefugte Einblick in Dokumente erhalten können, die nicht für sie bestimmt sind (Datenschutzgesetz, Betriebsgeheimnisse usw.).
- Netzwerkkabel, die durch öffentlich zugängliche Räume führen, sowie Modems und Netzwerkkomponenten in öffentlichen Räumen müssen speziell geschützt werden.

Nicht nur der Eingangsbereich, sondern auch Hintertüren und Parterrefenster müssen gesichert sein, damit ein unbefugtes Eindringen verhindert werden kann.

Schritt 10:
Mehr Sicherheit dank Ordnung



Ordnung ist nicht nur das halbe Leben, sondern auch ein zentraler Aspekt für die Sicherheit von Daten.

Hat Ordnung etwas mit Sicherheit zu tun? Mehr, als man auf den ersten Blick vielleicht meinen möchte. Ganz abgesehen von der Zeitersparnis, die ein aufgeräumter, ordentlicher Arbeitstisch bietet, gehen Informationen und Dokumente weniger verloren, wenn die Arbeitsfläche nicht mit Papieren, Handzetteln und Mäppchen übersät ist. Die Gefahr, dass sensible Dokumente im ungünstigsten Augenblick auftauchen oder von Unbefugten durch Zufall gelesen werden, wird so von Anfang an minimiert. Und denken Sie daran, Ordnung ist auch eine Frage des Images: Als Kunde oder Lieferant schliesst man vom ordentlichen Äussern bei einem Unternehmen gern auf die innere Haltung.

Massnahmen für bessere Ordnung

- Für elektronische Daten und die Aufbewahrung von Papierdokumenten ist ein Ablagesystem einzuführen, das alle einhalten müssen – z.B. Ablage nach Kunden, Projekten.
- Das Ablagesystem muss logisch aufgebaut und so gestaltet sein, dass es von den Mitarbeitenden verstanden und auch konsequent angewendet werden kann (siehe Schritt 8).
- Eine saubere Übergabe von Arbeiten und Dokumenten bei Ferienabwesenheiten verhindert, dass Mitarbeiter in den Unterlagen oder Computern ihrer Kollegen stöbern und so durch Zufall auf Informationen stossen, die nicht für sie bestimmt sind.
- Als Grundlage für mehr Sicherheit sind ausreichend Schränke, Korpusse, Ordner usw. zur Verfügung zu stellen.
- Während Pausen und bei Abwesenheit vom Arbeitsplatz sollte der Computer gesperrt werden, damit Unbefugte keinen Einblick auf die bearbeiteten Dokumente haben. Wer mit sensiblen Daten arbeitet, schliesst sein Büro ab.
- Nicht mehr benötigte Papierdokumente und Notizen mit sensiblen Daten müssen sicher vernichtet werden (Aktenvernichter). Sie gehören weder in den Abfall noch ins Altpapier.
- Nicht mehr benötigte elektronische Daten auf Speichermedien wie Disketten, CDs und DVDs müssen sicher gelöscht und mehrfach überschrieben werden. Mit Microsoft Windows ist dies nicht möglich, der einfache Löschbefehl reicht also nicht aus! Nicht mehr benötigte Speichermedien mit sensiblen Daten werden deshalb physisch zerstört.
- Werden Speichermedien ausser Haus gegeben, sind dafür neue, noch nie verwendete Datenträger einzusetzen. Konventionell gelöschte Informationen können leicht wiederhergestellt und von Unbefugten gelesen werden.
- Ordner mit Personaldaten, Verträgen und Offerten gehören unter Verschluss, damit es nicht zu Verstössen gegen das Datenschutzgesetz kommt.
- Wer mit sensiblen Daten am Computer arbeitet, positioniert seinen Bildschirm so, dass Kollegen und Besucher die Informationen nicht lesen können.

Glossar

Applikation Anwendungsprogramm, z.B. ein Textverarbeitungs- oder ein E-Mail-Programm.
ADSL Sehr schneller Internetzugang. Bei ADSL ist der Computer bzw. der Server permanent mit dem Internet verbunden und Hackerangriffen somit dauernd ausgesetzt – Firewall einsetzen!
Attachment Anhang, an eine E-Mail angehängte Datei. Viele bösartige Programme werden in solchen Anhängen verbreitet und durch das Öffnen des Attachments aktiviert.
Backup Wörtlich Rückendeckung, im IT-Zusammenhang Sicherung von Daten, Programmen und Programmkonfigurationen.
Betriebssystem Systemsoftware oder Systemprogramme. Gruppe meist kleinerer Programme, die beim Start des Computers geladen werden und ihn betriebsbereit machen.
Browser Software, die es gestattet, von Servern im Internet Informationen abzurufen.
Download Wörtlich «herunterladen», gemeint ist das Herunterladen von Programmen und Dateien aus dem Internet.
Firewall Wörtlich Brandschutzmauer, Gerät oder Sicherheitsprogramm, das die Verbindung ins Internet sichert und ein Netzwerk oder einen einzelnen Computer vor unbefugtem Zugriff von ausserhalb des Netzwerks schützt.
ISDN Digitales Fernmeldenetz zur Übertragung von Telefon, Fax und Daten mit Übertragungsraten von 64 bzw. 128 KB pro Sekunde. Im Vergleich mit der analogen Technik verbesserte Übertragungsqualität und -sicherheit.
Modem Elektronisches System, das zur Aufbereitung und/oder Umwandlung elektrischer Signale für Senden und Empfang in Kommunikations-Netzwerken verwendet wird und den Internetzugang über die Telefonleitung ermöglicht.
Patch Wörtlich Pflaster, Aktualisierung von Betriebssystemen und Anwendungsprogrammen (Update).
Provider Anbieter eines Internetzugangs, z.B. Bluewin, Sunrise, Cablecom, Green.ch.
Remote Access Zugriff von ausserhalb auf das firmeneigene Netzwerk. Die Berechtigung für Remote Access ist zeitlich zu limitieren, die Aktivitäten von Personen mit Remote Access müssen überwacht werden.
Router Gerät, welches Netzwerke untereinander verbindet.
Server Computer, der seine Hardware- und Software-Ressourcen in einem Netzwerk anderen Rechnern zugänglich macht, z.B. Applikations-, Daten-, Web-, Mail-Server.
Spam Massen-E-Mail, analog zu den Kettenbriefen, die früher per Post verschickt wurden. Gegen Spam hilft ein Spamfilter.
Trojaner, trojanisches Pferd Schädlicher Programmteil. Wird üblicherweise als Bestandteil einer E-Mail oder beim Herunterladen einer Datei unbemerkt auf dem Rechner abgespeichert. Unter vorgegebenen Bedingungen aktiviert es sich auf dem befallenen Computer und sammelt, manipuliert oder zerstört Daten. Moderne Form von Spionage und Sabotage.
Update Aktualisieren eines Programms (Patch).
URL Adresse einer Seite im Internet, z.B. www.infosurance.ch.
USB-Stick Speichermedium, das in den USB-Anschluss gesteckt wird. Dank seiner Kleinheit und der riesigen Speicherkapazität (bis zu 1 GB) ein Gerät, das gerne in der Wirtschaftsspionage eingesetzt wird.
Virus Verstecktes, schädliches Programm, das Daten zerstört. Kann durch jede Form der Datenübernahme (Internet, Disketten, CDs, Netzwerke usw.) übertragen und verbreitet werden – Antivirus-Programm einsetzen.
VPN Abkürzung für Virtual Private Network, Netzwerk aus virtuellen Verbindungen (z.B. via Internet), über welche Daten sicher (verschlüsselt) übertragen werden. Dank VPN können die verschiedenen Zweigstellen eines Unternehmens kostengünstig und abhörsicher miteinander kommunizieren.
Wurm Von einer Datei unabhängiges, schädliches Programm, das sich unter Ausnutzung von Schwachstellen durch Kopieren von einem Rechnersystem oder -netzwerk zum nächsten ausbreitet. Meistens enthält ein Wurm Befehle, die Daten direkt zerstören oder die Systemleistung beeinträchtigen.