

Mehr Informationssicherheit für KMU (Teil 1)

Text André Schmid*

Bilder Doris Gerber

Haben Sie sich schon einmal überlegt, ob in Ihrem Betrieb die Kernleistungen erbracht werden können, wenn das Computernetzwerk plötzlich nicht funktioniert? Unabhängig davon, ob in Ihrem Betrieb hundert oder bloss drei Computer im Einsatz stehen, als Mitglied der Geschäftsleitung sollten Sie sich periodisch mit dieser Frage auseinander setzen. In einer zweiteiligen Folge wird hier das Vorgehen anhand von zweimal fünf Schritten dargestellt.



Die wichtigen Geschäftsdaten sollen gegen bösartige Attacken geschützt sowie sicher verwahrt und behütet werden.

Auch ein Betrieb, der seinen einzigen Computer nur dazu benutzt, um Rechnungen zu schreiben und gelegentlich eine E-Mail zu versenden, hat die gesetzliche Aufbewahrungspflicht von Geschäftsdaten zu erfüllen und den Datenschutz einzuhalten. Für einen unbeabsichtigten Verstoß gegen die gesetzlichen Auflagen reicht oft ein eingeschlepptes Virus oder eine schlecht gewartete Firewall. Schlimmer noch, schädliche Computerprogramme können zum unwiederbringlichen Verlust wichtiger Geschäftsdaten führen und so Ihr Unternehmen in seiner wirtschaftlichen Existenz gefährden.

Ein Computerabsturz kann teuer werden

Datenverluste und Computersysteme, die durch bösartige Attacken aus dem Internet zusammenbrechen, können für die verantwortliche Geschäftsleitung kostspielig werden – insbesondere weil die Zahl der Angriffe auf Firmennetzwerke in den vergangenen Jahren dramatisch zugenommen hat und Schutzmassnahmen heute zu einem absoluten Muss geworden sind. Wer nicht dafür besorgt ist, dass in seinem Betrieb ausreichende Schutzvorkehrungen umgesetzt werden, lebt riskant.

Das Thema Informationssicherheit wird für alle Unternehmen immer bedeu-

tender. Bereits heute verlangen Anbieter von Geschäftsversicherungen von ihren Kunden im Sicherheitsbereich immer mehr proaktives Handeln bis hin zum Nachweis von Vorkehrungen zur Informationssicherheit. Es zahlt sich also aus, wenn Sie dieses Thema regelmässig in den Geschäftsleitungssitzungen thematisieren und diskutieren.

10 Schritte zu mehr Informationssicherheit

Wie Sie die Sicherheit und den Bestand Ihres Unternehmens, die Verfügbarkeit Ihrer Daten und Informationen nachhaltig verbessern und sich vor bösartigen Angriffen von innen und aussen schützen können, erfahren Sie auf den folgenden Seiten. Ziel des 10-Punkte-Programms von InfoSurance ist es, Sie bei der Einführung eines wirkungsvollen Grundschutzes zu unterstützen, damit in Zukunft der Verlust von vitalen Geschäftsdaten verhindert werden kann und bei einem Systemausfall der finanzielle Schaden möglichst gering bleibt.

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

Schritt 1: Managementaufgaben wahrnehmen – Verantwortlichkeiten zuteilen



Klare Verantwortlichkeit: Es ist ein interner oder externer IT-Verantwortlicher zu bezeichnen, der dafür sorgt, dass die anfallenden Sicherheitsaufgaben seriös durchgeführt und kontrolliert werden.

Die besten Sicherheitslösungen, die motiviertesten Mitarbeiter können nur dann zu einem wirkungsvollen Grundschutz beitragen, wenn auch die Geschäftsleitung ihren Beitrag zu mehr Sicherheit leistet.

Bestimmen Sie in Ihrem Unternehmen, auch wenn Sie nur zwei Personen beschäftigen, einen EDV- bzw. IT-Verantwortlichen sowie einen Stellvertreter. Ist das nötige Wissen für diese Aufgabe nicht vorhanden, schicken Sie Ihre Mitarbeitenden in einen entsprechenden Kurs oder arbeiten Sie mit einem externen IT-Sicherheitsexperten zusammen. Ein dreitägiger Lehrgang oder eine externe Fachperson kommt Ihr Unternehmen wesentlich günstiger zu stehen als die Folgen eines Datenverlustes oder ein Verstoß gegen das Datenschutzgesetz.

Alle Sicherheitsaufgaben, die an den internen IT-Verantwortlichen und an externe Personen delegiert werden, wie z.B. das Erstellen von Backups, sind schriftlich zu erteilen und in einem Pflichtenheft festzuhalten (siehe unten). Kontrollieren Sie regelmässig, ob der IT-Verantwortliche die ihm übertragenen Aufgaben korrekt ausführt.

Sämtliche Mitarbeitenden, die an einem Computer tätig sind, erhalten ein Benutzungsreglement, das beschreibt, welche Aktionen auf dem Computer durchgeführt werden dürfen und welche untersagt sind (siehe Schritt 8).

Aufgaben eines IT-Verantwortlichen

Zu den Aufgaben eines internen oder externen IT-Verantwortlichen gehören unter anderem:

- Regelmässige Datensicherung bei Servern, Clients (Arbeitsstationen), Notebooks (tragbaren Computern)

und anderen mobilen Geräten (siehe Schritt 2)

- Aktualhalten von Antivirus-Programm, Firewall, Betriebssystem und sonstiger Software (siehe Schritte 3, 4 und 5)
- Führen einer Liste mit allen im Unternehmen vorhandenen Computern, den darauf installierten Programmen sowie den ausgeführten Software-Aktualisierungen (siehe Schritt 5)
- Verwalten der Zugriffsrechte: Welche Programme darf der einzelne Mitarbeitende ausführen? Auf welche Daten hat er Zugriff?
- Führen und Aktualhalten einer Liste mit allen Personen, die Remote Access (Zugriff von aussen) auf das Firmennetzwerk haben – unter anderem genaue Dauer der Berechtigung festlegen und diese nach Ablauf entziehen. Sorgen Sie dafür, dass die Schutzprogramme auf den externen Computern aktuell gehalten werden.
- Sicherstellen, dass es zu keinen Verletzungen des Datenschutzgesetzes kommt – unter anderem durch das Aktualhalten der diversen Schutzprogramme (Firewall, Virenschutz) und das Verwenden von starken Passwörtern (siehe Schritte 3, 4 und 7)
- Kontrollieren, dass die Mitarbeitenden die IT-Richtlinien einhalten (siehe Schritt 8)
- Ansprechpartner sein für Sicherheitsfragen bzw. Meldestelle bei sicherheitsrelevanten Vorkommnissen (z.B. bei Verlust von Notebooks, bei festgestellten Viren usw.) →

Schritt 2: Backup: Daten regelmässig sichern und richtig archivieren

Nicht nur Hacker und Viren bedrohen Ihre Geschäftsdaten. Auch Gefahren wie Feuer, Wasser oder Kurzschlüsse können im Schadensfall zum Totalverlust von wichtigen Informationen führen – eine doppelt unangenehme Situation, denn auch der Gesetzgeber verlangt, dass Geschäftsdaten aufbewahrt und archiviert werden. Der Verlust von Betriebsdaten ist daher unbedingt zu verhindern. Daten müssen deshalb regelmässig gespeichert, sicher archiviert und die Backups periodisch getestet werden.

Sorgen Sie dafür, dass elektronische Daten regelmässig auf einem beweglichen Speichermedium wie Band, CD oder DVD gespeichert werden. Die Häufigkeit der Datensicherung richtet sich nach der Tätigkeit und der Grösse Ihres Unternehmens. Die komplette Sicherung aller Daten muss im Minimum einmal pro Woche, bei grösseren Betrieben täglich durchgeführt werden.

Regeln Sie schriftlich, wer die Datensicherung ausführt und wie häufig dies zu geschehen hat. Führen Sie eine Kontrollliste, in der die erfolgte Datensicherung eingetragen werden muss (siehe Schritt 1, Pflichtenheft IT-Verantwortlicher).

Gesichert werden alle im Unternehmen bearbeiteten Daten, d.h. sämtliche Files (Dateien), Briefe, Tabellen und E-Mails mit geschäftsrelevantem Inhalt. Idealerweise wird auch von der Softwarekonfiguration ein Backup gemacht. So wird bei einem Totalausfall der Computersysteme wertvolle Zeit gespart, weil die Software schneller wieder installiert werden kann.

Wichtig: Wochen-, Monats- und Jahres-Backups dürfen nicht im Betrieb aufbewahrt werden, da sie bei Wasser-

einbrüchen oder Feuer ebenfalls zerstört werden können. Empfohlener Aufbewahrungsort für Sicherungskopien ist ein Banksafe oder bei Ihnen zu Hause.

Prüfen Sie regelmässig, ob sich Ihre Sicherungskopien noch lesen lassen.

Beispiel für einen Betrieb mit täglichem Backup

- Tages-Backup: Für die Tage Montag bis Donnerstag wird je ein Speichermedium verwendet. Die Tageskopien werden jeweils am entsprechenden Wochentag in der folgenden Woche überschrieben (sofern das Speichermedium ein Überschreiben zulässt). Die Tageskopien werden im Betrieb, aber ausserhalb des Serverraums aufbewahrt.
- Wochen-Backup: Für jeden Freitag im Monat ist ein separates Speichermedium zu verwenden und ausserhalb des Betriebs aufzubewahren. Die Wochenkopien werden jeweils am entsprechenden Freitag im folgenden Monat überschrieben.
- Monats-Backup: Jeweils Ende Monat wird eine Monatskopie erstellt. Die Monats-Backups werden nicht mehr überschrieben und ausserhalb des Betriebs aufbewahrt.
- Jahres-Backup: Jeweils Ende Jahr wird eine Jahreskopie erstellt. Das Jahres-Backup wird nicht mehr überschrieben und ausserhalb des Betriebs aufbewahrt. →



Von den Daten muss regelmässig ein Backup gemacht werden. Die dazu verwendeten Datenträger sind sicher zu verwahren, z.B. in einem feuerfesten Tresor ausserhalb des Betriebs.

Schritt 3: Antivirus-Programm installieren und aktuell halten



Stichwort Prophylaxe: Was für den Menschen eine Grippeimpfung, ist für den Computer das Antivirus-Programm.

Internet und E-Mail sind Kommunikations- und Informationsmittel, die aus dem modernen Geschäftsalltag nicht mehr wegzudenken sind. Schädliche Programme wie z.B. Viren können diese Kommunikationsinfrastrukturen lahm legen und die wirtschaftliche Existenz eines Unternehmens gefährden. Neben dem direkten Schaden werden unzureichend geschützte Computersysteme häufig zur Verbreitung von Viren und für gezielte Attacken gegen ein drittes Unternehmen missbraucht. Wer als Geschäftsleiter ungenügende Vorkehrungen zum Schutz seiner Computersysteme trifft, handelt fahrlässig und muss allenfalls sogar mit Strafverfolgung rechnen.

Computerviren können Daten und Programme verändern, manipulieren oder sogar vollständig zerstören. Bösartige Computerprogramme werden via E-Mail-Anhänge (Attachments) und Speichermedien wie Disketten usw. übertragen. Im Internet sind Viren oft als nützliche oder unterhaltende Gratisprogramme getarnt, die durch einen simplen Mausklick aktiviert werden.

Den einzigen Schutz vor bekannten Viren bietet ein Antivirus-Programm, das gefährliche Eindringlinge identifiziert und unschädlich macht. Die entsprechenden Programme können in Computerläden gekauft oder kostenlos aus dem Internet heruntergeladen werden.

Da Hacker dauernd neue Viren programmieren, muss das Antivirus-Programm laufend aktualisiert werden. Je nach Produkt, das Sie verwenden, sucht sich das Programm auf der Website des Herstellers selbstständig die verfügbaren Aktualisierungen. Informieren Sie sich bei Ihrem Verkäufer, ob

dies bei Ihrem Programm der Fall ist. Falls dies nicht so ist, sollte die Aktualisierung jede Woche, besser noch jeden Tag durchgeführt werden.

Damit Ihr Netzwerk zuverlässig vor Viren und anderen schädlichen Programmen geschützt ist, muss das Antivirus-Programm auf sämtlichen Servern und Arbeitsstationen (Clients) installiert und regelmässig aktualisiert werden. Bei grösseren Netzwerken werden das Antivirus-Programm und die Aktualisierungen am besten zentral und automatisch betrieben.

«Virus-Scans», d.h. das Absuchen der Harddisk nach Viren, sind im Minimum einmal wöchentlich durchzuführen, damit unerkannt eingeschleppte Viren entdeckt und eliminiert werden können. Bei regem Datenaustausch und bei Verdacht auf ein Virus empfiehlt sich ein täglicher Virus-Scan.

Nicht vergessen: Werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen müssen vom IT-Verantwortlichen sofort geändert werden!

Tipps für die Mitarbeiter-IT-Richtlinien (siehe auch Schritt 8):

- Eingegangene Virus-Warnungen müssen unverzüglich dem IT-Verantwortlichen gemeldet und nicht etwa Kollegen und Bekannten weitergeleitet werden.
- Das Ausschalten des Antivirus-Programms ist ausdrücklich untersagt.
- Tests, wie und ob das Antivirus-Programm im Ernstfall funktioniert, sind ausdrücklich verboten. →

Schritt 4: Ins Internet nur mit Firewall – keine Chance für unbefugten Zugriff



So, wie eine Brandmauer das Übergreifen eines Feuers von einem Gebäude zum Nachbargebäude verhindert, sorgt eine Firewall dafür, dass Unbefugten der Zugriff auf ein Computersystem verwehrt wird.

Gibt es in Ihrem Betrieb Brandschutztüren? Wenn ja, dann achten Sie bestimmt darauf, dass diese Türen auch stets geschlossen werden. In der Welt des Internets und des elektronischen Datenaustauschs ist es die Firewall, die diese Sicherheitsaufgabe erfüllt. Ohne Firewall können Unbefugte auf Ihren Computersystemen Befehle ausführen, an Geschäftsgeheimnisse und Daten gelangen, die dem Datenschutzgesetz unterstehen, oder auch Ihre Rechner zu illegalen Attacken auf Dritte missbrauchen.

Installieren Sie eine Firewall. Sorgen Sie dafür, dass der Internetzugang ausschliesslich über die Firewall erfolgen kann (siehe unten). Für Firmennetzwerke ist eine Hardware-Firewall, für mobile Geräte (Notebooks) eine Software-Firewall zu empfehlen. Im Handel sind Produkte erhältlich, die gleichzeitig eine Firewall und einen Virenschutz bieten. Gerade für kleinere Betriebe sind kombinierte Produkte sehr zu empfehlen.

Manche Betriebssysteme, z.B. Windows XP oder Mac OSX, haben eine Firewall eingebaut, die allerdings keinen vollständigen Schutz bietet. Nutzen Sie aber auf jeden Fall auch diese Möglichkeit und aktivieren Sie die Firewall.

Die Firewall muss regelmässig mit den neuesten Bedrohungsmustern aktualisiert und auf ihre Funktionsfähigkeit geprüft werden (Update – siehe Schritt 5).

Sämtliche Netzwerkübergänge müssen mit einer Firewall gesichert werden. Stellen Sie sicher, dass die Verbindungen zu Lieferanten, Kunden und Mitarbeitenden, die Fernzugriff auf Ihr Netzwerk haben, mit einer Firewall gesichert sind und diese Firewalls aktuell gehalten werden.

Wenn in Ihrem Betrieb Computer mit Wireless LAN (drahtlose Netzwerkverbindung) eingesetzt werden, dann sorgen Sie dafür, dass dies richtig und sicher getan wird (siehe Schritt 6). Falsch genutzte Wireless-LAN-Geräte machen den ganzen Schutz zunichte, den Ihnen Ihre Firewall bietet.

Falls der Zugang zur Konfiguration Ihrer Firewall mit einem Passwort geschützt werden kann, sollten Sie dies tun. Verwenden Sie dazu ein starkes Passwort (siehe Schritt 7). Es lohnt sich, die Konfiguration der Firewall zu speichern (siehe Schritt 2).

Tipps für Mitarbeiter-IT-Richtlinien

Der gesamte Internetverkehr wird über die Firewall abgewickelt. Aus Sicherheitsgründen ist es untersagt,

- auf anderen Wegen, z.B. via Modem, auf das Internet zuzugreifen,
- private Laptops und
- Wireless-LAN-Geräte im Unternehmen ohne schriftliche Einwilligung des IT-Verantwortlichen einzusetzen. →

Schritt 5: Software regelmässig warten und aufdatieren

Kontrollieren Sie bei Ihrem Auto auch regelmässig Ölstand und Reifendruck? Sorgen Sie bei abgenutzten Bremsbelägen dafür, dass diese rechtzeitig ersetzt werden? Genau so, wie Sie Ihren Wagen aus Sicherheitsgründen regelmässig warten, müssen auch die Computerprogramme in einem Unternehmen periodisch gepflegt und auf den neuesten Stand gebracht werden.

Menschen machen Fehler – da Computerprogramme von Menschen geschrieben werden, gibt es auch keine fehlerfreien Computerprogramme. Aus diesem Grund bieten die Hersteller regelmässig Software-Aktualisierungen an, so genannte «Updates» oder «Patches».

Sorgen Sie dafür, dass die neuesten Patches für Betriebssysteme und Appli-

kationen (Anwendungsprogramme) bei Ihnen installiert werden. Installieren Sie nur Aktualisierungen für die von Ihnen tatsächlich verwendete Version des Betriebssystems (z.B. Windows XP) und die von Ihnen eingesetzten Anwendungsversionen (z.B. Internet Explorer 6).

Verfügbare Sicherheits-Updates sollten immer sofort installiert werden. Bei den übrigen, nicht sicherheitsrelevanten Updates empfiehlt es sich abzuklären – insbesondere wenn Sie Programme von verschiedenen Herstellern verwenden (z.B. Windows und SAP-Applikation) –, ob der neue Patch Störungen verursachen kann.

Sämtliche am Netzwerk angeschlossenen Computer müssen aufdatiert werden. Dies gilt auch für Notebooks und Geräte von externen Mitarbeitenden. Für jeden Computer ist eine Liste zu führen, welche Updates installiert sind.

Hier finden Sie die neuesten Updates für die gängigsten Produkte:

- Für Windows-Anwender:
www.windowsupdate.com
- Für Office-Anwender:
www.officeupdate.com

Die Schritte 6–10 werden in einer späteren applica publiziert.



Beim Auto wird der Ölstand kontrolliert, doch auch der Computer will regelmässig gewartet werden.