

10-Punkte-Programm der Informationssicherheit – ein Muss für KMU

Informationssicherheit ist in den KMU erfahrungsgemäss ein eher zweitrangiges Thema. Dies völlig zu unrecht, da die Ansprüche an die Verfügbarkeit und die Vertraulichkeit der Systeme meist viel höher sind, als auf den ersten Blick angenommen. Wie lange kann Ihr Unternehmen ohne IT-Infrastruktur weiterfunktionieren? Welches wären die Folgen, wenn vertrauliche Informationen in falsche Hände kämen?

■ Von Carlos Rieder

Oftmals wird gesagt, dass die KMU kein lohnendes Ziel für Hacker seien. Falsch! Hacker missbrauchen ungeschützte Systeme zur Durchführung ihrer Angriffe. Wer seine Systeme ungeschützt betreibt, macht sich somit zum Mittäter, vergleichbar mit dem Auto, das mit steckendem Zündschlüssel abgestellt wird. Bei einem Missbrauch haftet der Halter für entstandene Schäden mit.

Der Verein InfoSurance engagiert sich für die Informationssicherheit in der Schweiz. Die Arbeitsgruppe KMU der InfoSurance hat das so genannte 10-Punkte-Programm der Informationssicherheit erarbeitet. Dieses enthält die wichtigsten 10 Massnahmen, welche in einem Unternehmen umgesetzt werden

Tipps & Tricks zum Thema Passwörter

- Verwenden Sie keine Passwörter, die in Wörterbüchern zu finden sind.
- Verwenden Sie keine Passwörter, die Namen, AHV- und Passnummern und Geburtsdaten aus dem Familienumfeld enthalten.
- Prüfen Sie die Qualität eines Passwortes mit einem Passwort-Checker.
- Wechseln Sie das Passwort mindestens alle zwei Monate. Idealerweise wird dies vom System erzwungen.

müssen. Die Realisierung der Massnahmen ist einfach und führt bei minimalem Aufwand zu maximalem Nutzen!

Übersicht zum 10-Punkte-Programm:

1. Erstellen Sie ein Pflichtenheft für IT-Verantwortliche! Wer ist für welche Aufgabe der Informationssicherheit verantwortlich? Für die Datensicherung, für das Einspielen von Software-Updates, für die Vergabe von Zugriffsberechtigungen etc.

2. Sichern Sie Ihre Daten regelmässig mit Backups! Es muss sichergestellt werden, dass regelmässig eine vollständige Datensicherung stattfindet, idealerweise täglich. Backup-Medien sind extern zu lagern und müssen mindestens quartalsweise auf Lesbarkeit geprüft werden.

3. Halten Sie Ihr Antivirus-Programm aktuell! Der Einsatz eines Antivirus-Programms ist inzwischen zu einer Selbstverständlichkeit geworden. Damit diese Software ihre Aufgabe erfolgreich wahrnehmen kann, müssen jedoch die so genannten Viren-Signaturen (Fingerabdrücke der Viren) regelmässig aktualisiert werden. Nur so kann sichergestellt werden, dass stets auch neue Viren erkannt werden.

4. Schützen Sie Ihren Internetzugang mit einer Firewall! Die Mehrzahl der Hackerangriffe ist nur möglich, weil der Übergang vom internen Netzwerk zum Internet nicht

oder nur unzureichend mit einer Firewall geschützt ist. Ständig aktive Suchroboter finden automatisch schlecht geschützte Netzwerke und missbrauchen diese (z.B. auch für weitere Angriffe).

Tipps & Tricks zum Thema Wireless-LAN

- Ändern Sie den vom Hersteller vorgegebenen Namen für Ihr Wireless-LAN (Service Set ID – SSID). Die neue Identifikation darf keinesfalls Ihren Firmennamen enthalten.
- Deaktivieren Sie die SSID-Ausstrahlung, damit Ihr AccessPoint für Dritte nicht sichtbar ist.
- Aktivieren Sie die Verschlüsselung der kabellosen Datenübermittlung WEP (Wired Data Encryption). Wählen Sie die 128-Bit-Verschlüsselung.
- Ändern Sie das Standard-Passwort Ihres Access Points.
- Setzen Sie den MAC-Adressen-Filter ein, damit nur bekannte Geräte mit dem AccessPoint kommunizieren können.
- Übermitteln Sie hoch vertrauliche Daten nur über Verbindungen, welche zusätzlich mit einem Virtual Private Network (VPN) geschützt sind.



Vorsorge hilft vor Schäden zu schützen.

Richtlinien für die IT-Benutzerinnen und -Benutzer

- Regeln Sie die Installation und den Einsatz von eigenen Programmen und Hardware (Spiele, Bildschirmschoner, USB-MemorySticks, Modems, private Notebooks, Wireless-LAN, Handheld-Computer etc.).
- Regeln Sie den Gebrauch des Internets: Was dürfen die Mitarbeitenden herunterladen, was nicht (Informationen, Programme etc)?
- Untersagen Sie den Besuch von Chatrooms, aber auch von Webseiten mit pornografischen, rassistischen und gewaltverherrlichenden Inhalten.
- Legen Sie die Art und Weise der Datensicherung fest, v.a. bei den Notebookbenutzerinnen und -benutzern (siehe Punkt 2).
- Legen Sie den Umgang mit Passwörtern fest (siehe Punkt 6).
- Regeln Sie den Umgang mit Sicherheits-Updates und Antivirus-Programmen (siehe Punkt 3 und 5).
- Regeln Sie den Gebrauch von E-Mails: keine vertraulichen Daten, kein Weiterleiten an die private E-Mail-Adresse, keine Kettenbriefe etc.
- Legen Sie den Umgang mit vertraulichen Informationen und Daten fest und richten Sie eine geschützte Dateiablage ein.
- Regeln Sie das Verhalten bei sicherheitsrelevanten Vorkommnissen, z.B. Viruswarnungen, Diebstählen und Verlusten von Notebooks und Passwörtern.
- Kündigen Sie Sanktionen bei einem Verstoß gegen die Benutzerrichtlinien an.

5. Aktualisieren Sie Ihre Software regelmässig! Software muss wie ein Auto gewartet werden. Alle Hersteller bieten in regelmässigen Abständen Software-Updates oder Software-Patches an, welche erkannte Fehler korrigieren. Vor allem die sicherheitsrelevanten Updates müssen unter allen Umständen installiert werden.

6. Verwenden Sie starke Passwörter! Passwörter schützen Ihre «Computer-Identität» vor Missbrauch. Einfache Passwörter können von entsprechenden Programmen binnen Sekunden «erraten» werden. Gute Passwörter bestehen aus Zahlen, Buchstaben (klein und gross) und Sonderzeichen (z.B. Punkt, Komma) und sind mindestens 8 Zeichen lang.

7. Schützen Sie Ihre mobilen Geräte! PDAs, Palms und Smart-Phones haben sich zu kleinen Computern mit grossem Funktionsumfang entwickelt. Wie deren grosse Brüder, so müssen auch die mobilen Geräte mit Hilfe von Antivirus-Software geschützt werden. Besonderes Augenmerk sollte auch der Ver-

schlüsselung der Daten geschenkt werden, da das Verlustrisiko bei dieser Geräteklasse besonders hoch ist!

8. Machen Sie Ihre IT-Benutzerrichtlinien bekannt! Einfach anwendbare IT-Benutzerrichtlinien legen fest, was im Umgang mit der IT zulässig und was verboten ist. Die klar definierten Vorgaben helfen den Anwenderin-

nen und Anwendern, sich zu orientieren. Vermitteln Sie die Inhalte allen Mitarbeitenden nachvollziehbar und verständlich.

9. Schützen Sie die Umgebung Ihrer IT-Infrastruktur! Um die Verfügbarkeit der IT-Infrastruktur sicherzustellen, muss diese auch vor Feuer, Wasser und unerlaubtem Zugriff geschützt werden. Da viele Informationen in

Tipps & Tricks zum Thema Backup

- Erstellen Sie von Montag bis Donnerstag je ein Tages-Backup auf einem eigenen Speichermedium. Die Tages-Backups werden jeweils am entsprechenden Wochentag in der folgenden Woche überschrieben. Bewahren Sie die Tageskopien ausserhalb des Serverraums auf.
- Erstellen Sie jeden Freitag ein Wochen-Backup auf einem separaten Speichermedium und bewahren Sie dieses ausserhalb des Betriebs auf. Das Wochen-Backup wird nach einem Monat wieder überschrieben.
- Erstellen Sie am Monatsende das Monats-Backup. Das Monats-Backup wird nicht mehr überschrieben und ausserhalb des Betriebs aufbewahrt.
- Erstellen Sie Ende Jahr das Jahres-Backup. Das Jahres-Backup wird nicht mehr überschrieben und ebenfalls ausserhalb des Betriebs aufbewahrt.
- Überprüfen Sie periodisch, ob sich die Daten von den Sicherungsmedien zurückspielen lassen. Jede Sicherung ist nutzlos, wenn die Daten nicht korrekt auf das Backup-Medium übertragen wurden.



InfoSurance hat auf der Website auch einen Bereich für KMU.

Papierform vorliegen, muss unberechtigten Dritten auch der Zugang zu den Arbeitsplätzen verwehrt werden.

10. Halten Sie Ordnung in Ihren Dokumenten und Datenträgern! Dokumente und Datenträger werden auf einem ordentlichen Arbeitsplatz weniger leicht verlegt und müssen somit auch nicht lange gesucht werden. Das Wegschliessen vertraulicher Unterlagen verhindert die «zufällige» Einsicht durch Besucher oder das Reinigungspersonal.

Das ausführliche 10-Punkte-Programm ist unter www.infosurance.ch kostenlos abrufbar.

Umsetzung im Unternehmen

Die Umsetzung des 10-Punkte-Programms kann selbstständig oder in Zusammenarbeit mit einem IT-Partner erfolgen. Die Erfahrung zeigt, dass die Einführung schrittweise erfolgen sollte. Vor allem nichttechnische Massnahmen brauchen Zeit bis sie von allen

Mitarbeitenden mitgetragen werden. Im Weiteren ist es von grosser Wichtigkeit, dass das Management die Anstrengungen zur Verbesserung der Informationssicherheit unterstützt und mit gutem Vorbild voran geht.

Prozess

Die Informationssicherheit ist ein Prozess. Dieser muss immer wieder den aktuellen Gegebenheiten angepasst werden. Eine regelmässige Überprüfung der Wirkung der angeordneten Massnahmen ist für die Aufrechterhaltung der Informationssicherheit unabdingbar. Diese Aufgabe sollte nach Möglichkeit von unabhängigen Dritten wahrgenommen werden. Diese sind weniger betriebsblind und können somit Schwächen besser aufdecken.

Es tun!

Das richtige Anpacken des Themas Informationssicherheit bedeutet Arbeit! Wir sind jedoch der Meinung, dass sich der Aufwand

KMU-Roadshow – Sensibilisierungskampagne zur Informationssicherheit

Oftmals zeigen die KMU wenig Interesse an grossen, nationalen Sicherheitsveranstaltungen. Kostenlose Anlässe in den Regionen finden im Gegensatz dazu aber grossen Anklang. Gemeinsam mit Partnern will die InfoSurance verschiedene Anlässe verteilt über die gesamte Deutschschweiz durchführen. Dabei stellt die InfoSurance die Inhalte zur Verfügung (10-Punkte-Programm der Informationssicherheit, inklusive dazugehöriger Präsentationen und Referenten), und der Partner organisiert das Rahmenprogramm des Anlasses und lädt seine Kunden und andere interessierte Personen ein. Für die Durchführung der KMU-Roadshow werden noch Partner gesucht. Bitte wenden Sie sich bei Interesse an die Geschäftsstelle der InfoSurance (041 228 41 70, mail@infosurance.ch).

unbedingt lohnt. Die Risiken der IT werden kalkulierbarer und die Auswirkungen allfälliger Vorfälle kleiner. Starten Sie jetzt mit dem 1. Punkt, und legen Sie die Verantwortlichkeiten fest!

Tipps & Tricks für IT-Verantwortliche

- Sichern Sie die Daten auf Servern, Arbeitsstationen, Notebooks, Laptops und anderen mobilen Geräten regelmässig (siehe Punkt 2).
- Halten Sie Betriebssysteme, Antivirus-Programme, Firewalls und sonstige Software aktuell (siehe Punkte 3, 4 und 5).
- Ändern Sie werkseitige Passworteinstellungen bei Geräten, Betriebssystemen und Anwendungsprogrammen sofort.
- Führen Sie eine Liste mit allen im Unternehmen vorhandenen Computern, mit den installierten Programmen sowie den ausgeführten Software-Aktualisierungen (siehe Punkt 5).
- Legen Sie die Zugriffsrechte fest: Welche Programme dürfen Mitarbeitende ausführen? Auf welche Daten haben Mitarbeitende Zugriff?
- Führen Sie eine Liste mit allen Personen, welche von aussen auf das Firmennetzwerk zugreifen, eventuell mit genauer Dauer der Berechtigung. Stellen Sie sicher, dass auch deren Schutzprogramme aktuell sind.
- Stellen Sie sicher, dass Datenschutz-Bestimmungen eingehalten werden, z.B. durch aktuelle Schutzprogramme und starke Passwörter (siehe Punkte 3, 4, 6).
- Kontrollieren Sie regelmässig, ob die Benutzerrichtlinien eingehalten werden.

AUTOR

Carlos Rieder
Leiter Competence Center IT-Security
Hochschule für Wirtschaft HSW Luzern
Partner isec ag, Luzern
Präsident InfoSurance
Zentralstrasse 9, CH-6002 Luzern
Tel. +41 41 228 41 70
Fax +41 41 228 41 71

crieder@hsw.fhz.ch

ONLINE

www.hsw.fhz.ch/iwi