

office IT-Security

► Problemen in Unternehmen, die oft nicht erkannt, tabuisiert oder schlichtweg ignoriert werden:

- 40 Prozent der Internet-Nutzung im Office dient nicht beruflichen Zwecken.
- Die Hälfte aller Büroangestellten lädt Programme aus dem Internet herunter.
- 46 Prozent der Befragten haben schon mindestens einmal

persönliche Files (Musik, FunClips etc.) von USB-Sticks auf Arbeits-PCs überspielt.

● Mehr als die Hälfte aller Beschäftigten gaben an, dass sie Geschäftsdaten mitnehmen würden, wenn sie aus ihrem derzeitigen Unternehmen ausscheiden ...

Sorglosigkeit und fehlendes Wissen. Angesichts derart dramatischer Zahlen sollte man meinen, dass Unternehmen auf der Hut sind – die Mitarbeiter-Sicherheitsrichtlinien fallen aber oft trotzdem un-

zureichend aus. – Mehr als ein Drittel aller Betriebe hat gar keine Regeln und selbst dort, wo es welche gibt, sind sie einem Viertel der Beschäftigten unbekannt ...

Folgen der Misere. Neben den direkten finanziellen Verlusten durch Systemausfälle, verlorene Daten, unproduktive Mitarbeiter etc. beeinträchtigen Schadensfälle häufig auch Geschäftsbeziehungen und haben einen negativen Einfluß auf den allgemeinen Ruf eines Unternehmens.

Mögliche Lösungswege. Der Faktor „Mitarbeiter“ muss in alle Überlegungen zur Verbesserung der IT-Security mit einbezogen werden. Ein einfaches Sperren von USB-Ports sowie der Einsatz von Filter- und Überwachungs-Software allein reichen in der Regel nicht aus, da sie keine geeigneten Maßnahmen sind, um das Sicherheitsbewußtsein der Mitarbeiter zu sensibilisieren. Effektiven Schutz erreicht man aber nur, wenn den Beschäftigten die Risiken und Auswirkungen möglichen Fehlverhaltens bekannt sind.

Mitarbeiter brauchen höheres Sicherheits-Bewußtsein

Entscheidend ist es daher, ein klares Regulativ zu schaffen, das die private Internet- und E-Mail-Nutzung genauso festlegt wie den sicheren Umgang mit geschäftlichen Daten und die Sorgfaltspflicht bei der Verwendung von PCs.

Schnell-Check. Nicht nur Unternehmer, auch Mitarbeiter können dazu beitragen, das Sicherheitsrisiko im Betrieb zu reduzieren. – Die Checkliste links liefert wichtige Tipps. ■

kutscherauer.anton@e-media.at

Interview



DR. ANDREAS EUSTACCHIO
Experte für
Datenschutz-
& IT-Recht bei
Eustacchio &
Schaar Rechts-
anwälte

Sicherheitsregeln schützen Chefs und Mitarbeiter

E-MEDIA: Wie sollten Unternehmen der „Gefahr“ durch Mitarbeiter begegnen?

EUSTACCHIO: Entweder im Dienstvertrag oder in anderen Richtlinien sollten Regeln beim Umgang mit vertraulichen Daten, Computer und Internet definiert sein.

E-MEDIA: Welche Bereiche sollten diese Regeln auf alle Fälle umfassen?

EUSTACCHIO: Etwa die Verwendung externer Datenträger, Verschwiegenheits-Klauseln zu Betriebsgeheimnissen und klare Richtlinien zur privaten Nutzung des Internet-Zugangs in der Firma. Es ist auch ratsam, in Dienstverträgen für die Zeit nach dem Ausscheiden des Dienstnehmers Vorsorge zu treffen.

E-MEDIA: Mit welchen Konsequenzen müssen Mitarbeiter rechnen, die nachweislich Schaden angerichtet haben?

EUSTACCHIO: Bei mißbräuchlicher E-Mail-Nutzung können Kündigung oder Entlassung drohen. Bei Datenschutzvergehen legen Datenschutzgesetz und Strafgesetzbuch die Bestimmungen fest, die hohe Geld- & Freiheitsstrafen (bis 10 Jahre) zur Folge haben können. Auch die Störung von Computersystemen ist strafbar. Dabei genügt es, wenn der Täter eine schwere Störung ernstlich für möglich hält und sich damit abfindet (bedingter Vorsatz).

Checkliste für Mitarbeiter

Erfülle ich die wichtigsten allgemeinen gültigen IT-Sicherheitsrichtlinien?

JA PASSWÖRTER

- Wurden sichere Passwörter gewählt? (Groß-/Kleinbuchstaben, Ziffern, Sonderzeichen ...)
- Sind die Passwörter nicht älter als drei Monate?
- Werden Passwörter nicht weitergegeben?
- Wird ein eventuell notiertes Passwort sicher aufbewahrt?

SICHERER UMGANG MIT DEM COMPUTER

- Ist ein Schutz vor unbefugtem Zugriff auf IT-Systeme bei Abwesenheit vorhanden?
- Wurde der Kennwortschutz des Bildschirmschoners aktiviert und auf zehn Minuten eingestellt?
- Sind alle Sicherheitsupdates für das Betriebssystem und die Anwendungen auf dem aktuellsten Stand (wurden immer alle akzeptiert und das System baldmöglichst neu gestartet ...?)
- Sind Antiviren-Tools aktiviert und die Virendefinitionen aktuell?
- Wurden IT-Systeme nicht eigenmächtig verändert?
- Wird nur von der Unternehmens-IT genehmigte Software genutzt?

NUTZUNG VON E-MAIL/INTERNET

- Herrscht verantwortungsvoller Umgang mit E-Mail und Internet (geschäftliche/private Nutzung)?
- Wird bei E-Mails von unbekanntem Absendern, mit unerwarteten Inhalten risikobewusst vorgegangen?
- Checkt man den Spamordner regelmäßig auf False-Positives?
- Wurden etwaige Phishing-Attacken an Helpdesk/Admin gemeldet?
- Ist die Standard-Sicherheitseinstellung z. B. des Internet-Browsers nicht verändert worden?
- Werden vertrauliche E-Mail-Anhänge verschlüsselt und die Passwörter nicht per E-Mail zum Empfänger übermittelt?

UMGANG MIT MOBILEN GERÄTEN

(Notebooks, PDAs, Handys, USB-Sticks)

- Ist der Schutz vor unbefugtem Zugriff und Diebstahl gewährleistet, ein Laptop-Schloss („Kensington“) angebracht?
- Sind PDA, Handy, etc. bei Nicht-Benutzung gesperrt?
- Ist die Bluetooth-Funktion beim Handy ausgeschaltet?
- Werden USB-Sticks und andere Speicher sicher aufbewahrt?
- Werden regelmäßig Backups durchgeführt?