5 Security-Tipps für kleine Unternehmen

1. Backups. Erstellen Sie regelmäßig Sicherheitskopien Ihrer Daten auf einer externen Festplatte. Im Falle eines Systemabsturzes können diese weitestgehend wiederhergestellt werden. Ein Backup-Server ermöglicht eine zentrale Speicherung aller Netzwerkzweige.

2. Verschiedene angemessene Passwörter. Überlegen Sie sich für jeden passwortgeschützten Bereich, auf den Sie zugreifen, ein gesondertes Passwort. Je komplexer die Passwörter sind, desto schwieriger können sie von Hackern geknackt werden.

Komplexität. Vermeiden Sie leicht durchschaubare Zeichenfolgen wie Namen, häufige Phrasen oder Nummernfolgen. Von „iloveyou“, „test“ oder „1234“ ist unbedingt abzuraten. Die Sicherheit eines Passworts steigt, je mehr Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen (z. B. Rauten) es enthält. Es sollte dabei keine Struktur erkennbar und somit keine Durchschaubarkeit vorhanden sein.

Reine Kopfsache. Sehen Sie unbedingt davon ab, Passwörter auf Notizen sichtbar zu hinterlegen oder in Smartphones zu speichern. Im Falle eines Verlustes sind derart dokumentierte Passwörter gefundenes Fressen für Datendiebe. Um sich Ihre Passwörter zu merken, können Sie beispielsweise als Groß- und Kleinbuchstaben die Anfangsbuchstaben verschiedener Wörter eines Satzes verwenden. Sofern sich das Notieren nicht umgehen lässt, sollten Sie darauf achten, die Passwörter an einem Ort zu verwahren, auf den nur Sie zugreifen können.

Die Menge macht‘s. Bedenken Sie, dass Ihre Identität auf sämtlichen von Ihnen genutzten Internetportalen zur freien Verfügung für Angreifer steht, sofern Sie nur ein Passwort für alle Aktivitäten nutzen. Je mehr Passwörter Sie verwenden, desto besser ist Ihre Identität geschützt, da der Schaden im Falle eines Datenverlusts begrenzt wird. Im Idealfall verwenden Sie jeweils ein Passwort für jedes Portal, das Sie betreten.

3. Leitlinien für Soziale Netzwerke. Soziale Netzwerke wie Facebook oder Twitter sind für viele Menschen ein wichtiger Bestandteil der Unternehmenskommunikation geworden – und dieser Trend setzt sich fort. Leider ist dies auch zu Cyberkriminellen durchgedrungen, so dass mittlerweile solche Plattformen ein beliebtes Ziel für Malware- und Phishing-Angriffe darstellen. Da die Aktivität in Sozialen Netzwerken zum Unternehmenserfolg beitragen kann, ist es nicht im Sinne des Erfinders, die Benutzung der Netzwerke zu unterbinden. Stattdessen sollten innerhalb des Unternehmens Leitlinien für die Benutzung der Netzwerke vereinbart werden, die von jedem Mitarbeiter unterschrieben werden. Da es unter Umständen schwierig ist, die dortigen Sicherheitseinstellungen optimal zu konfigurieren, sollten Sie Ihre Mitarbeiter darin schulen.

4. Richtiger Umgang mit E-Mails. Auch wenn in den meisten E-Mail-Programmen ein Spam-Filter integriert ist, sollten Sie vorsichtig im Umgang mit E-Mails sein. Des Öfteren kursieren E-Mails, deren Absender sich als Online-Banken oder Ähnliches ausgeben und zum Teil gefährlich gut als solche getarnt sind – nicht nur in den Augen des Empfängers, sondern auch für den Filter. Unter einem Vorwand fordern diese E-Mails dazu auf, auf einer Seite, zu der im selben Zug weitergeleitet wird, persönliche Zugangsdaten wie Benutzername und Passwort einzugeben. Dieses Vorgehen wird als Phishing bezeichnet.

Seriöse Anbieter werden Sie niemals nach Ihren Zugangsbeziehungsweise Kontodaten fragen oder zu einer Eingabe ebendieser auffordern. Sollten Sie einer solchen E-Mail begegnen, sollten Sie sie löschen. Es ist allgemein Vorsicht geboten, sobald ein Link in einer E-Mail enthalten ist — insbesondere dann, wenn der Inhalt der Mail in einer fremden Sprache verfasst ist. Weitere Spam-Anzeichen sind pharmazeutische, sexuelle oder temporär beliebte Themen (zum Beispiel Weihnachtsgrüße, Naturkatastrophen oder Prominente) sowie Lockbotschaften („Sie haben gewonnen!“). Lassen Sie sich nicht davon beeindrucken, wenn Ihnen der Absender zunächst bekannt erscheint. Angreifer verfügen über Mittel und Wege, ihre Absender-Adresse zu anonymisieren beziehungsweise in eine für den Angriffszweck passende zu verwandeln.

5. Schutz der Server und Endgeräte. Bei aller Vorsicht, die Sie als Anwender walten lassen, ist ein automatisierter Schutz Ihrer Server und Endgeräte nicht zu vernachlässigen. Eine gute Sicherheitslösung lässt sich individuell an Ihre Bedürfnisse anpassen und hilft Ihnen unter anderem dabei, den Schutz Ihrer Netzwerk-Infrastruktur zentral zu verwalten, Ihre Unternehmensleitlinien unkompliziert umzusetzen, nicht mehr benötigte Dateien endgültig zu löschen und sensible Inhalte wie persönliche Kontodaten zu verbergen.

www.kaspersky.com/de