

Keine Chancen für Viren und Hacker – die zehn goldenen Regeln

Die „zehn goldenen Regeln der Informationssicherheit in KMU“, herausgegeben durch InfoSurance, die Stiftung für einen sicheren Informations- und Kommunikationsplatz Schweiz, sind einfach gehalten und auch für KMU leicht umzusetzen.

Die meisten Massnahmen zur Erhöhung der Informationssicherheit sind weniger eine Frage der Kosten als vielmehr des Willens, sie in einem Unternehmen tatsächlich umzusetzen. Speziell für alle KMU hat die Stiftung InfoSurance zehn Regeln der Informationssicherheit zusammengestellt, welche wir Ihnen hier kurz vorstellen möchten:

Diese Sicherheitsregeln sollten die Benutzerin und der Benutzer sensibilisieren und die Informationen zusammengestellt.

1. Verantwortlichkeit

Wer für Datensicherung, Updates, Antivirus und andere Software zuständig und Ansprechpartner für Sicherheitsfragen ist, muss klar festgehalten sein.

2. Datensicherung

Von allen variablen Daten sollten regelmässig Sicherungen erstellt werden. Diese Backups sind an einem separaten Ort aufzubewahren, damit sie beispielsweise nach einem Brandfall noch verfügbar sind.

3. Schutz vor Computerviren

Die Antivirensoftware muss zwingend auf allen Systemen installiert sein. Sie gehört zu einer der wichtigsten Software in einer Unternehmung. Wichtig ist, dass der Virenschutz mindestens im wöchentlichen Turnus auf den neusten Stand gebracht wird. Deshalb ist es zwingend notwendig, dass man ein aktualisierbares Virenprogramm auswählt.

4. Sichere Verbindung ins Internet

Bei unzureichendem Schutz können Daten von aussen manipuliert werden. Deshalb ist eine Firewall – eine elektronische Brandmauer – notwendig, die zwischen PC, Server, Netzwerk

und dem Internet steht und den Schutz für die Daten gewährleistet.

5. Softwareaktualisierung / Patches

So genannte „Patches“ helfen, Softwarefehler und unerwartetes Verhalten von Software, die sich erst in der Praxis zeigen, zu beheben. Diese „Patches“ stellen die Hersteller zur Verfügung.

6. Umgang mit Passwörtern

Passwörter sollten mindestens 8 Stellen umfassen und aus Zahlen, kleinen Buchstaben und Sonderzeichen zusammengesetzt sein. Und: Passwörter machen nur Sinn, wenn sie persönlich und geheim bleiben.

7. Zutrittsregelung

Für sämtliche Räume, in denen sich IT-Infrastrukturen befinden, sind Zutrittsregelungen und Überwachung notwendig. EDV Arbeitsplätze und Druckerstationen in öffentlichen zugänglichen Zonen sind zu vermeiden.

8. Benutzerrichtlinien

Klar und einfach formulierte Richtlinien definieren für alle Benutzerinnen und Benutzer den Umgang mit der IT-Infrastruktur. Ergänzende Schulungen sind in vielen Fällen sinnvoll.

9. Sensibilisierung

Damit Massnahmen im Rahmen der Informationssicherheit nicht vergessen gehen, ist die regelmässige Sensibilisierung der Mitarbeiter notwendig.

10. Ordnung

Eine systematische Ablage von physischen und elektronischen Daten sowie die regelmässige Archivierung und Entsorgung schonen nicht nur Ressourcen und Nerven, sondern tragen auch zur Informationssicherheit bei.