Achtung Cyber-Risiko! Zehn Tipps zum Schutz Ihrer Office-IT

Jedes vierte mittelständische Unternehmen wurde bereits Opfer eines Hackers. Das ist das Ergebnis einer Forsa-Befragung im Auftrag des Gesamtverbands der Deutschen Versicherungswirtschaft (GDV). Einige dieser Angriffe wären vermeidbar gewesen. Schon durch einfache Schutzmaßnahmen lässt sich die Sicherheit erheblich erhöhen. Wir haben zehn Tipps für Sie zusammengestellt, um Sie bei der Absicherung Ihrer Office-IT zu unterstützen.

1. Realistisches Risikobewusstsein aufbauen
Viele Betriebe schätzen das Cyber-Risiko zwar allgemein als hoch ein, halten sich selbst aber – oft irrtümlich – für kein interessantes Ziel. Ein Trugschluss, der sich nachteilig auf die IT-Sicherheit auswirkt.

2. Starke Passwörter technisch erzwingen
„1235“ und „Passwort“ sind eine Einladung für Hacker. Erzwingen Sie im ganzen Unternehmen starke Passwörter. Für mehr Passwortsicherheit sorgt ein Passwortmanager oder eine Zwei-Faktor-Authentifizierung.

3. Wöchentliche Sicherungskopien machen
Mit Sicherungskopien lassen sich durch einen Angriff verlorene Daten schnell wiederherstellen. Machen Sie mindestens einmal wöchentlich ein Backup und testen Sie, ob Ihre Sicherungskopie auch funktioniert.

Zusatztipp: Bewahren Sie Ihre Backups physisch getrennt vom gesicherten System auf. So haben Sie auch bei Diebstählen oder einem Brand noch Zugriff auf alle Daten.

4. Auf Sicherheitslücken schnell reagieren

Laufend werden Datenlecks wie Collection#1 bekannt oder es wird über neue Sicherheitslücken und Softwarelösungen berichtet. Handeln Sie unverzüglich und prüfen Sie, ob Ihre Systeme auch betroffen sind.

5. Sicherheitsupdates sofort installieren
Die meisten Softwarehersteller veröffentlichen regelmäßig Updates, um publik gewordene Sicherheitslucken zu schließen. Schieben Sie die Installation dieser wichtigen Updates also nicht auf die lange Bank!

6. Sorgfalt bei den Administratoren-Rechten
Jeder Mitarbeiter mit Administratoren-Rechten ist ein potentielles Sicherheitsrisiko! Vergeben Sie daher solche Rechte nur sehr sparsam und wirklich nur an die Personen, die sie zwingend benötigen.

7. Mobile Geräte zusätzlich absichern
Laptops, Tablets und Smartphones können gestohlen werden und in falsche Hände geraten. Achten Sie daher bei allen mobilen Geräten besonders sorgfältig auf eine sichere Datenverschlüsselung.

8. Server mit 2-Faktor-Authentifizierung sichern
Da Server in der Regel ständig über das Internet erreichbar sind, sind sie ein sehr beliebtes Angriffsziel für Hacker. Sichern Sie Ihre Server bestmöglich ab – mit einer 2-Faktor-Authentifizierung.

9. Benutzerindividuelle Kennungen
Statten Sie ausnahmslos jeden Nutzer, der Zugang zu Ihren Systemen hat, mit einer eigenen Zugangskennung und individuellem Passwort aus. So kann nachvollzogen werden, wer das System wann verwendet hat.

10. Schutz gegen Schadsoftware
Ein Virenscanner bietet zwar keinen 100%igen Schutz, filtert aber einiges an Schadsoftware heraus. Mindestens einer sollte daher installiert sein und – ebenso wie die Firewall –

regelmäßig aktualisiert werden.

Zusatztipp: Die meisten Angriffe erfolgen per E-Mail! Sensibilisieren Sie Ihre Mitarbeiter für diese Gefahr und führen Sie fortwährend Schulungen zum Thema E-Mail-Sicherheit durch.

DIE VSMA GMBH: UNTERSTÜTZUNG IM KAMPF GEGEN CYBER-RISIKEN

Sie fühlen sich der wachsenden Bedrohung durch Cyber-Angriffe nicht gewachsen? Wir helfen weiter. Als 100%iges Tochterunternehmen des VDMA e.V. bietet Ihnen die VSMA GmbH kostenlose Publikationen mit Handlungsleitfäden und Tipps für den Ernstfall sowie ein Online-Tool zur Prüfung Ihres Cyber-Risikos. Gemeinsam mit dem VDMA haben wir außerdem eine speziell auf die Anforderungen des Maschinen- und Anlagenbaus ausgerichtete Cyber-Versicherungslösung entwickelt. Fragen? Wir beraten Sie gerne!

- **Branchenversicherung VDMA Cyber-Police: https://cyber.vsma.de**
- **Cyber-Risiko-Prüfung: https://www.vsma.de/vdma-cyber-risiko-pruefung**
- **Broschüre "Tipps für den Cyber-Schadenfall": https://cyber.vsma.de**
- **Video „Cyberrisiken im Maschinen- und Anlagenbau": https://cyber.vsma.de**

Beitragsbild: NicoElNino / iStock

Kontakt:
Herr Thomas Völker
VSMA GmbH – ein Unternehmen des VDMA
Telefon +49 69 6603-1520
tvoelker@vsma.org

VDMA Cyber-Police