HANDLUNGSEMPFEHLUNG

Schutz sensibler Unternehmens-daten & Apps vor Verlust & Zugriff

ORBIT IT-SOLUTIONS

Unsere 5 Handlungsempfehlungen für Ihre Security Roadmap

... kurzfristig

1 SPF, DKIM und DMARC:

Richten Sie die Authentifizierungsmechanismen für Ihren Mailversand ein. Ein geringer Aufwand bringt großen Nutzen: Sie sorgen dafür, dass Ihre E-Mails weiterhin bei Ihren Empfänger*innen ankommen, weil Sie durch die Authentifizierung als Absender als vertrauenswürdig und Ihre Mails als sicher eingestuft werden. Ohne die Mechanismen werden Ihre Mails blockiert.

2 Exchange:

Spielen Sie immer die aktuellen Updates ein, um die Angriffsfläche für Cyberattacken zu minimieren. Der Exchange Server ist ein sehr kompatibler Mailserver (für das Microsoft-Umfeld) und das meistverbreitete Mailsystem der Welt. Das macht ihn besonders attraktiv für Cyberangriffe.

3 Data-Loss-Prevention-Richtlinien:

Schützen Sie Ihre Daten, indem Sie unerlaubte Datenzugriffe und unzulässiges Löschen von Daten verhindern. Bestimmen Sie, welches Maß an Schutz Ihre Daten benötigen und entwickeln Sie eine Richtlinie, ggf. mit Unterstützung eines Tools.

... mittelfristig

4 Datenklassifizierung:

Identifizieren und klassifizieren Sie sensible Daten. Kennzeichnen Sie ausgehende E-Mails, ob diese öffentlich, intern oder vertraulich sind. Dateien sollten Sie nicht mehr per E-Mail verschicken, sondern per Link mit Externen teilen. Hier können Sie granular die Berechtigungen für die geteilten Daten definieren und verhindern eine ungewollte Weitergabe.

5 Awareness & Trainings:

Schulen Sie Ihre Mitarbeitenden! Nur wenn diese sensibilisiert, sich den Gefahren bewusst und darin geschult sind, können Sie Angriffe durch Spam und Phishing vermeiden. Simulieren Sie reale Angriffe, bieten Sie Mikrolernen und kontinuierliche Weiterbildungen, um auf der sicheren Seite zu sein.