

Tipps zur Cybersicherheit für KMU

Da Unternehmen zunehmend auf Automatisierungstechnik setzen, vergrößert sich die potenzielle Angriffsfläche für Cyber-Bedrohungen. Auch wenn kleine und mittlere Unternehmen nicht unbedingt über die Ressourcen größerer Player verfügen, müssen auch sie in ihre Sicherheitsinfrastruktur investieren. Hier drei Tipps:

1



Schulen Sie Ihre Mitarbeiter

Die Schulung sollte die folgenden Elemente umfassen:

- Wie man sichere Passwörter verwendet
- Woran man bösartige E-Mails erkennt
- Wie man bei der Telearbeit sein WLAN-Heimnetzwerk schützt
- Wie man sensible bzw. vertrauliche Unternehmensdaten schützt
- Wie man eine Cyberbedrohung erkennt und meldet

2



Implementieren Sie eine Firewall

Für KMU eignet sich am besten eine Hardware-Firewall mit Software-Kontrollen, die als Teil eines Sicherheitssystems fungiert, das Unterstützung für virtuelle private Netzwerke (VPN), Antivirus-, Antispyware- und Content-Filter-Funktionen beinhaltet.

3



Optimieren Sie Ihre Cloud-Strategie

Wählen Sie Cloud-Plattformen und -Anwendungen, die das höchste verfügbare Sicherheitsniveau bieten und über integrierte Sicherheitsmechanismen zum Schutz vor Schwachstellen verfügen.

Dabei sind die wichtigsten Überlegungen:

- Zugänglichkeit, Rückverfolgbarkeit und Sicherheit
- Skalierbarkeit – Cloud-Systeme müssen einfach nach oben oder unten skaliert werden können, um sich an die Geschwindigkeit des Unternehmenswachstums anzupassen.

Eine Cloud-Strategie kann Datensicherung und Disaster Recovery übernehmen und erfordert lediglich eine einmalige Investition ohne weitere Kosten.

Denken Sie daran, dass eine erfolgreiche Cybersicherheitsstrategie **proaktiv und nicht reaktiv** sein sollte. Das bedeutet, dass Unternehmen in die richtige Lösung investieren sollten, bevor etwas passiert, und nicht als Reaktion darauf, wenn etwas passiert ist.

