Best Practices in Bezug auf Sicherheit

In der heutigen Welt der vernetzten Geräte sind die folgenden Überlegungen zu beachten. Sie zu kennen, ist der erste Schritt. Das Befolgen dieser sinnvollen Best Practices bei allen vernetzten Geräten ist der nächste Schritt. Verwenden Sie diese Checkliste als Planungshilfe.

1. Früh anfangen

Planen Sie neue Technologie und ihren Schutz ein.

2. Daten schützen

Verwenden Sie verschlüsselte und authentifizierte Verbindungen, sofern vorhanden.

3. Dienste steuern

Deaktivieren Sie Technologiedienste, wenn Sie nicht vorhaben, sie zu verwenden.

4. Passwörter ändern

Die Verwendung von Standard-Passwörtern erleichtert Hackern den Zugriff auf Geräte. **Aktivieren Sie Passwörter für Benutzeroberflächen.**

5. Remote-Management

Verwenden Sie ein sicheres Remote-Managementsystem, um Einstellungen schnell aktualisieren zu können. Je länger Geräte, Lösungen und Systeme veraltete Einstellungen verwenden, desto höher ist das Risiko von Angriffen.

6. Aktivitätsprotokolle aktivieren

Verwenden Sie Aktivitäts- und Prüfprotokolle, um Fehlverhalten zu erkennen.

7. Kenntnis nur bei Bedarf

Auf Update-Pläne sollten nur diejenigen Zugriff haben, die sie benötigen. Wenn zu viele Mitarbeiter über Update-Pläne informiert sind, sind Verletzungen der Datensicherheit wahrscheinlicher.

8. Auf nicht mehr verfügbare Geräte achten

Entwickeln Sie eine Methode, um Geräte zu erkennen, zu denen die Verbindung abgebrochen ist. Wenn Sie den Verdacht haben, dass ein Gerät abhanden gekommen ist, sperren Sie die Anmeldedaten, bis Sie wissen, wo es sich befindet.

9. Aktualisierbarkeit

Wählen Sie Geräte, die während ihres Lebenszyklus aktualisiert werden können, um mit neuen Standards konform zu sein. Stellen Sie sicher, dass an der Update-Datei keine unbefugten Änderungen vorgenommen werden können.

10. Außerbetriebnahme von Geräten

Planen Sie die Außerbetriebnahme von Geräten, indem Sie Systemeinstellungen, Benutzerkonten und Anmeldedaten löschen und sicherstellen, dass alte Geräte in vorhandenen Systemen nicht fest codiert sind.

11. Datenschutz, Integrität und Verfügbarkeit

Beachten Sie Datenschutz, Integrität und Verfügbarkeit in allen Phasen des Lebenszyklus von Geräten.

12. Kontinuierliche Planung

Aktualisieren Sie die Sicherheitsrichtlinien regelmäßig. Die Planung der Sicherheit ist kein einmaliger Vorgang.

Wussten Sie schon?

360.000 USD

Verschlüsselung verringert die Kosten einer Datenpanne im Schnitt um **360.000 USD** und ist somit die effektivste Hacking-Gegenmaßnahme.[1]

81 %

Auf gestohlene oder schwache Passwörter waren **81 %** der durch Hacker verursachten Datenpannen zurückzuführen.[2]

1,2 Mio. USD

Unternehmen, die über IT-Notfallspezialisten verfügen und Reaktionspläne testen, reduzieren die Kosten von Datenpannen um mehr als **1,2 Mio. USD**.[3]

38 %

38 % der Firmen meldeten Sicherheitsvorfälle bei Unternehmensgeräten.[4]

40 %

40 % geben an, dass Cyberangriffe ein Grund sind, weshalb die Sicherung mobiler Geräte wichtig ist.

197 Tage

Es dauert durchschnittlich 197 Tage, bis Unternehmen eine Datenpanne bemerken.[5]

[1] Cost of a Data Breach Report 2019, IBM Security • [2] 2017 Verizon Data Breach Investigations Report, IBM Security • [3] Cost of a Data Breach Report 2019 • [4] Carbon Black Incident Response Threat Report, November 2018 • [5] 2018 und 2019 Cost of Data Breach, Ponemon Institute