CloudCommand

Cyber Security

CloudCommand GmbH chr.schumacher@gmx.tm

Cyber Security im Unternehmens-umfeld

CloudCommand GmbH chr.schumacher@gmx.tm

Mobile Device Security

Definition Mobile Device Security

Mobile Device Security bezieht sich auf die Maßnahmen, die entwickelt wurden, um sensible Informationen auf Laptops, Smartphones, Tablets, Wearables und anderen tragbaren Geräten zu schützen, die gespeichert und übertragen werden. Das Hauptziel besteht darin, zu verhindern, dass nicht autorisierte Benutzer auf das Unternehmensnetzwerk zugreifen können.

Mobilgeräte als Gefahrenquelle

Datenverlust und -diebstahl:

- Wenn ein Mitarbeiter sein Mobilgerät verliert oder es gestohlen wird, können vertrauliche Unternehmensdaten, Kundeninformationen und Geschäftsgeheimnisse gefährdet sein, wenn die Geräte nicht ausreichend geschützt sind.

Unsichere Apps:

- Mitarbeiter könnten unsichere Apps herunterladen, die Malware oder Spyware enthalten. Diese Apps können auf Unternehmensdaten zugreifen und sie stehlen oder beschädigen.

Mobilgeräte als Gefahrenquelle

Phishing und Betrug:

- Phishing-Angriffe können auf Mobilgeräten genauso effektiv sein wie auf Desktop-Computern. Mitarbeiter könnten betrügerische E-Mails oder Nachrichten erhalten und sensible Informationen preisgeben.

Unsichere Netzwerke:

- Wenn ein Mitarbeiter sein Mobilgerät verliert oder es gestohlen wird, können vertrauliche Unternehmensdaten, Kundeninformationen und Geschäftsgeheimnisse gefährdet sein, wenn die Geräte nicht ausreichend geschützt sind.

Mobilgeräte als Gefahrenquelle

Schwache Authentifizierung:

- Wenn mobile Geräte eine schwache Authentifizierung verwenden (z. B. einfache Passwörter oder keine Bildschirmsperre), können sie leichter von unbefugten Benutzern entsperrt werden.

Vertraulichkeitsverletzung:

- Unvorsichtige Mitarbeiter könnten vertrauliche Informationen auf Mobilgeräten speichern und versehentlich freigeben, indem sie sie an falsche Empfänger senden.

Mobile Strategy

Bring Your Own Device (BYOD):

- Mitarbeiter verwenden eigene Geräte

Choose Your Own Device (CYOD):

- Mitarbeiter dürfen sich Geräte selbst aussuchen.

Company-Owned, Personally Enabled (COPE):

- Firmeneigene, persönlich sowie beruflich genutzte Geräte

Company-Owned, Business-Only (COBO):

- Unternehmenseigene, ausschließlich geschäftlich nutzbare Geräte

Bring Your Own Device (BYOD)

VORTEILE	NACHTEILE
Kosteneffizienz: Unternehmen sparen Geld, da sie keine Geräte kaufen müssen.	**Sicherheitsrisiken:** Schwierige Trennung von persönlichen und geschäftlichen Daten kann Sicherheitsprobleme verursachen.
Mitarbeiterzufriedenheit: Mitarbeiter verwenden ihre bevorzugten Geräte, was zu höherer Zufriedenheit führen kann.	**Support-Herausforderungen:** IT-Abteilungen müssen eine Vielzahl von Geräten und Plattformen unterstützen.
Flexibilität: Mitarbeiter können an ihren eigenen Geräten arbeiten, was die Produktivität steigern kann.	**Datenschutzbedenken:** Unternehmen haben möglicherweise eingeschränkte Kontrolle über persönliche Daten auf den Geräten der Mitarbeiter.

Choose Your Own Device (CYOD)

VORTEILE	NACHTEILE
Sicherheitskontrolle: Unternehmen behalten die Kontrolle über die von ihnen ausgewählten Geräte.	**Höhere Kosten:** Das Unternehmen muss Geräte bereitstellen, was zu zusätzlichen Kosten führt.
Flexibilität: Mitarbeiter können aus einer vorab genehmigten Liste von Geräten wählen.	**Potenzielle Unzufriedenheit:** Mitarbeiter könnten mit den auswählbaren Geräten weniger zufrieden sein.
Sicherheitsbewusstsein: Unternehmen können Sicherheitsrichtlinien besser durchsetzen.	**Datenschutzbedenken:** Unternehmen haben möglicherweise eingeschränkte Kontrolle über persönliche Daten auf den Geräten der Mitarbeiter.

Corporate-Owned, Personally-Enabled (COPE)

VORTEILE	NACHTEILE
Volle Kontrolle: Unternehmen besitzen und kontrollieren die Geräte vollständig	**Höhere Kosten:** Unternehmen müssen die Geräte kaufen und verwalten.
Trennung von Geschäfts- und Privatdaten: Geschäftsdaten sind gut von persönlichen Daten isoliert.	**Eingeschränkte Mitarbeiterwahl:** Mitarbeiter haben normalerweise weniger Auswahlmöglichkeiten für persönliche Geräte.
Sicherheit: Unternehmen können Sicherheitsrichtlinien streng durchsetzen.	**Potenziell geringere Mitarbeiterzufriedenheit:** Mitarbeiter können sich in ihrer Gerätewahl eingeschränkt fühlen.

Corporate-Owned, Business-Only (COBO)

VORTEILE	NACHTEILE
Höchste Sicherheit: Unternehmen haben volle Kontrolle über die Geräte und Daten.	**Höhere Kosten:** Unternehmen müssen die Geräte kaufen und verwalten.
Trennung von Geschäfts- und Privatdaten: Geschäftsdaten sind strikt von persönlichen Daten getrennt.	**Eingeschränkte Mitarbeiterwahl:** Mitarbeiter haben normalerweise keine Wahl bei der Geräteauswahl für die Arbeit.
Sicherheit und Compliance: Unternehmen können strenge Sicherheits- und Compliance-Anforderungen erfüllen.	**Mögliche Unzufriedenheit:** Mitarbeiter könnten sich in ihrer Gerätewahl eingeschränkt fühlen und ihre persönliche Nutzung beeinträchtigt sehen.

CloudCommand

CloudCommand GmbH chr.schumacher@gmx.tm