HANDLUNGSEMPFEHLUNG

Verbindung von Identitäten & Endpunkten für einen Modern Secure Workplace

ORBIT IT-SOLUTIONS

Unsere 7 Handlungsempfehlungen für Ihre Security Roadmap

… kurzfristig

1 **Authentifizierungsmethoden:**

Über Multi-Faktor-Authentifizierung (MFA) verifizieren Sie sämtliche Zugriffe, um den Schutz zu erhöhen.

2 **Endgeräteverwaltung:**

Integrieren Sie alle Endgeräte in ein Verwaltungstool, damit Sie diese monitoren, zentral verwalten und Compliance-Richtlinien einhalten können.

3 **Endgeräteschutz:**

- **lokal:** Richten Sie auf dem einzelnen Endgerät einen Schutz-Agenten ein, z. B. mit vorgefertigten Richtlinien.
- **global:** Über eine Signalübermittlung wird der Schutzmechanismus aktiv, sobald ein Angriff erkannt wird.

4 **Conditional Access:**

Conditional-Access-Regeln im Rahmen Ihres festgelegten Identity Managements definieren, wer wann mit welchem Gerät auf welche Anwendungen zugreifen darf. Richten Sie Conditional Access in Azure oder On-Prem am Proxy ein.

… mittelfristig

5 **User-Rechteverwaltung:**

Nutzen Sie Identity- und Access-Management (IAM) und/oder User Access Management (UAM), um Benutzer*innenberechtigungen in Echtzeit an die Situation angepasst entziehen oder erlauben zu können.

6 **User Lifecycle:**

Etablieren Sie Prozesse, die bei einem Abteilungswechsel oder Austreten einer*s Mitarbeiter*in die Zugriffsberechtigungen entsprechend anpassen.

7 **IDTR – Identity Threat Detection and Response:**

Erhalten Sie Echtzeitreaktionen anhand von Risiko- und Verhaltensbewertung, indem Sie den Schutz von Identitäten und Endgeräten miteinander kombinieren.

ORBIT Gesellschaft für Applikations- und Informationssysteme mbH | mailing@orbit.de | www.orbit.de