BLUE CONSULT.

Sicherheitscheck für Entra ID / M365

Schließen Sie Ihre Sicherheitslücken, bevor es zu spät ist: Azure & Microsoft 365 im Fokus!?

Sichern Sie Ihre IT-Landschaft – Analysieren Sie Ihre Azure Umgebung

Cyberangriffe und Datenverluste sind für Unternehmen existenzbedrohend. Schwachstellen in der IT-Sicherheit können zu hohen finanziellen Verlusten, Imageschäden und rechtlichen Konsequenzen führen. Besonders bei Cloud-Diensten wie **Microsoft Azure** ist es entscheidend, Sicherheitslücken frühzeitig zu erkennen und zu schließen. Oftmals reichen kleinste Schwachstellen in der Sicherheitsarchitektur aus, um unbefugten Zugriff auf sensible Daten zu ermöglichen.

Regelmäßige Sicherheitsüberprüfungen sind unverzichtbar, um Ihre **Geschäftskontinuität** und **Compliance-Vorgaben zu erfüllen** und **zu sichern**. Nur durch gezielte Analysen können potenzielle Schwachstellen aufgedeckt und notwendige Maßnahmen ergriffen werden, bevor es zu spät ist.

Tägliche Angriffe: Microsoft berichtet, dass Kunden ihrer Cloud täglich mehr als **600 Millionen Cyberangriffen** ausgesetzt sind. Diese reichen von Phishing über Ransomware bis hin zu Identitätsdiebstahl

Passwortdiebstahl-Versuche: Hacker versuchen **4.000 Mal pro Sekunde**, Passwörter zu stehlen, was das enorme Ausmaß der Bedrohung verdeutlicht.

Diese Daten zeigen, wie dringend es ist, Cyberabwehrmaßnahmen zu verstärken und Sicherheitslücken zu schließen, insbesondere bei der Nutzung von Cloud-Diensten wie Microsoft Azure.

Quellen: Microsoft, TechRepublic

PIXABAY

Wie ist die Lage bei Ihnen?

- Ist Ihr Entra ID optimal konfiguriert, um Angriffe abzuwehren?
- Nutzen Sie alle verfügbaren Sicherheitsfeatures, die Microsoft 365 bietet?
- Wissen Sie, welche Schwachstellen und potenziellen Sicherheitslücken in Ihrer Azure Umgebung vorhanden sind?
- Haben Sie bereits Maßnahmen zur Absicherung Ihrer Benutzer und Cloud-Anwendungen implementiert?

Wenn Sie bei einer dieser Fragen unsicher sind, ist es an der Zeit, Ihre Azure Sicherheit zu überprüfen und zu verbessern. Regelmäßige Sicherheitsüberprüfungen, wie in unserem Workshop angeboten, sind daher unerlässlich, um diesen Bedrohungen einen Schritt voraus zu bleiben.

Microsoft Entra ID – früher Azure Active Directory (Azure AD) – ist eine Cloud-basierte Lösung für Identitäts- und Zugriffsverwaltung. Sie ermöglicht die Steuerung des Zugriffs auf Anwendungen und den Schutz von Identitäten. Aufgrund der umfangreichen Funktionen und unterschiedlichen Unternehmensanforderungen kann dies jedoch komplex werden, weshalb Expertise erforderlich ist, um alle Aspekte eines sicheren Identitäts- und Zugriffsmanagements zu berücksichtigen.

Unser Angebot:
Entra ID & Microsoft 365 Security Analyse / Workshop

Wir bieten eine umfassende, toolgestützte Analyse Ihrer Azure- und Microsoft 365-Umgebung, um Schwachstellen zu identifizieren und Optimierungspotenzial aufzuzeigen. Sie erhalten klare, praxisnahe Handlungsempfehlungen zur Verbesserung Ihrer Infrastruktur und Cloud-Sicherheit.

- **Ganzheitliche Überprüfung:** Unsere Microsoft-zertifizierten Experten analysieren Ihre Umgebung und liefern fundierte Erkenntnisse zu Sicherheitslücken, Leistungsengpässen und Optimierungsmöglichkeiten.
- **Individuelle Empfehlungen:** Auf Ihre Unternehmensanforderungen abgestimmte Vorschläge helfen Ihnen, Schwachstellen gezielt zu beheben und Ihre Azure-Strategie zu optimieren.
- **Für alle Erfahrungslevel:** Unser flexibler Ansatz passt sich an jedes Erfahrungslevel und Unternehmensstrukturen an, um eine effiziente Nutzung Ihrer Ressourcen sicherzustellen.
- **Workshop-Details:** Die Analyseergebnisse präsentieren wir im Rahmen des Workshops und geben Ihnen konkrete Maßnahmen zur Sicherheitsoptimierung.

Optionales Angebot:
Auf Wunsch erstellen wir ein maßgeschneidertes Angebot zur Umsetzung der empfohlenen Sicherheitsmaßnahmen.

Mit gezielten Analysen und der professionellen Bewertung durch unser erfahrenes Team unterstützen wir Sie dabei, **Ihre Ressourcen optimal zu nutzen und so eine maximale Effizienz Ihrer Azure- und Microsoft 365-Infrastruktur zu erreichen.**

Wir heben Ihre Sicherheitsmaßnahmen auf das nächste Level und erarbeiten praktikable Lösungen.

Benefits

- Sie erhalten einen umfassenden Überblick über den Sicherheitszustand Ihrer Azure Umgebung.
- Konkrete Handlungsempfehlungen und Priorisierungen helfen Ihnen, die richtigen Maßnahmen zu ergreifen.
- Durch die Beseitigung von Schwachstellen schützen Sie Ihre Daten und senken das Risiko von Cyberangriffen.
- Sie erfüllen regulatorische Anforderungen und sichern den Schutz sensibler Daten.

Warum BLUE?
Wir bieten einen umfassenden Lösungsansatz, der sowohl technische als auch organisatorische Aspekte einbezieht. Dazu ein klar strukturiertes Vorgehen durch definierte Workshop-Formate und bewährte Best Practices. Unser Team besteht aus zertifizierten Experten mit umfangreichem Wissen durch zahlreiche, erfolgreich abgeschlossene Kundenprojekte.

Kontakt

René Angenheister, Adolf-Dembach-Str. 2, 47829 Krefeld
experten@blue-consult.de, Telefon: +49 2151 6500 10

BLUE CONSULT.