BLUE CONSULT.

Conditional Access Design

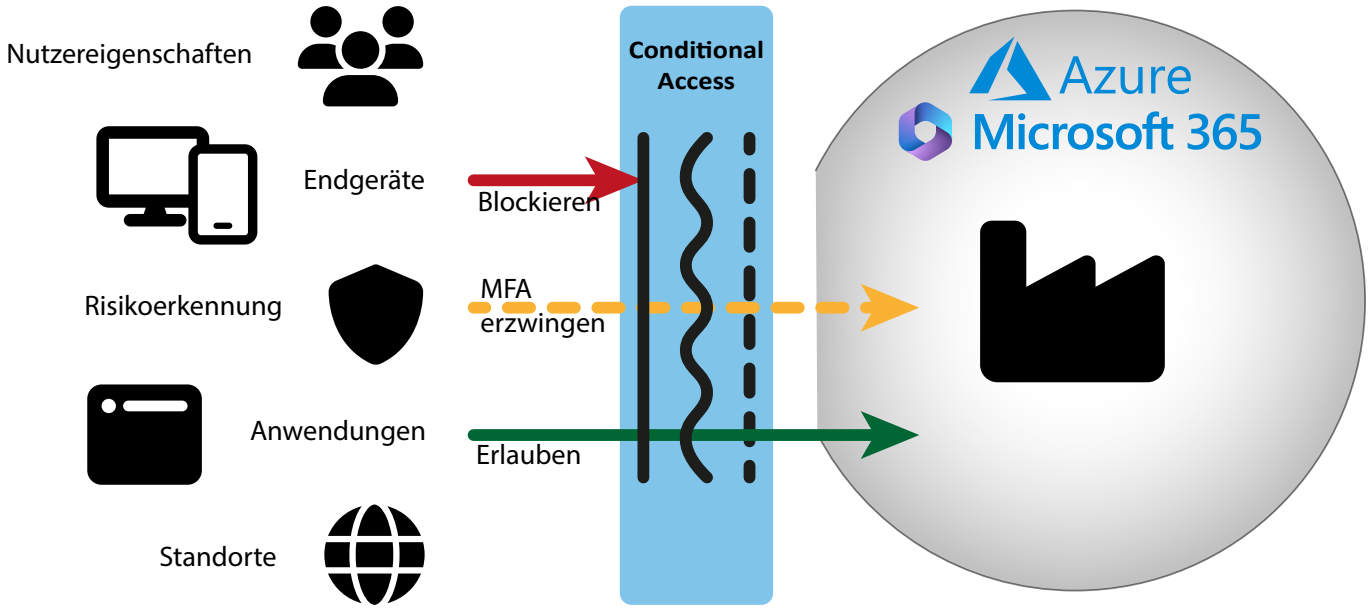
Conditional Access Design - denn Multi Factor Authentifizierung war gestern

Conditional Access für den modernen Arbeitsplatz: Schutz und Kontrolle

In unserer digitalisierten Arbeitswelt gewinnt Conditional Access zunehmend an Bedeutung, da die Cloud traditionelle Netzwerkgrenzen auflöst. Nutzer können unabhängig vom Gerät und von überall auf Daten und Anwendungen zugreifen und zusammenarbeiten – ein wesentlicher Vorteil des Modern Workplace. Dank Conditional Access behalten Sie die Kontrolle darüber, wer, mit welchem Gerät und unter welchen Bedingungen auf Ihre Cloud-Ressourcen zugreifen kann. So schützen Sie sensible Unternehmensdaten effektiv durch die Verwaltung von Identitäten und Endgeräten.

Was ist Conditional Access?

Um sich als Unternehmen vor Cyberangriffen zu schützen, bietet Microsoft Entra ID die Funktion Conditional Access. Diese ermöglicht es, den Zugriff auf Cloud-Daten zu regulieren, eine Multi-Faktor-Authentifizierung zu verlangen oder den Zugriff sogar zu verweigern, wenn bestimmte Bedingungen nicht erfüllt sind.



Wie ist die Lage bei Ihnen?

- Wissen Sie, mit welchen Geräten auf die Ressourcen zugegriffen wird und können Sie sicherstellen, dass diese unter Kontrolle sind?
- Können Sie sicherstellen, dass der Zugriff auf Ressourcen nur über zusätzliche Multifaktorauthentifizierung stattfindet, oder alternativ von definierten Quellen?
- Möchten Sie, dass Gastkonten unkontrollierten Zugriff auf Ressourcen haben?
- Möchten Sie, dass Administratorkonten von Service Providern unkontrollierten Zugriff auf Ressourcen haben?
- Möchten Sie, dass Dienstkonten oder Konten von Partnern unkontrollierten Zugriff auf Ressourcen haben?

Angebot BLUE:

Wir bieten Ihnen eine Analyse der zentralen Verwaltung von Regelwerk und Zugriffsparametern, um sicherzustellen, dass Ihre Cloud-Daten bestmöglich geschützt sind. Unser Angebot umfasst folgende Schritte:

- Analyse: Wir überprüfen den Ist-Zustand. Ist ein Conditional Access Regelwerk vorhanden und auf welchem Niveau ist es implementiert.
- Vergleich mit Best Practices und den BLUE-Erfahrungen: Anschließend vergleichen wir Ihr Regelwerk mit unseren Best Practises und Erfahrungen und erörtern gemeinsam die notwendigen Änderungen zur Verbesserung der Sicherheitsrichtlinien.
- Einführung des „BLUE-Standard“-Regelwerks: Wir unterstützen Sie bei der Implementierung des neuen Regelwerks und starten mit einem anfänglichen Monitoring. Die schrittweise Aktivierung der neuen Sicherheitsmaßnahmen erfolgt in enger Zusammenarbeit mit Ihnen.

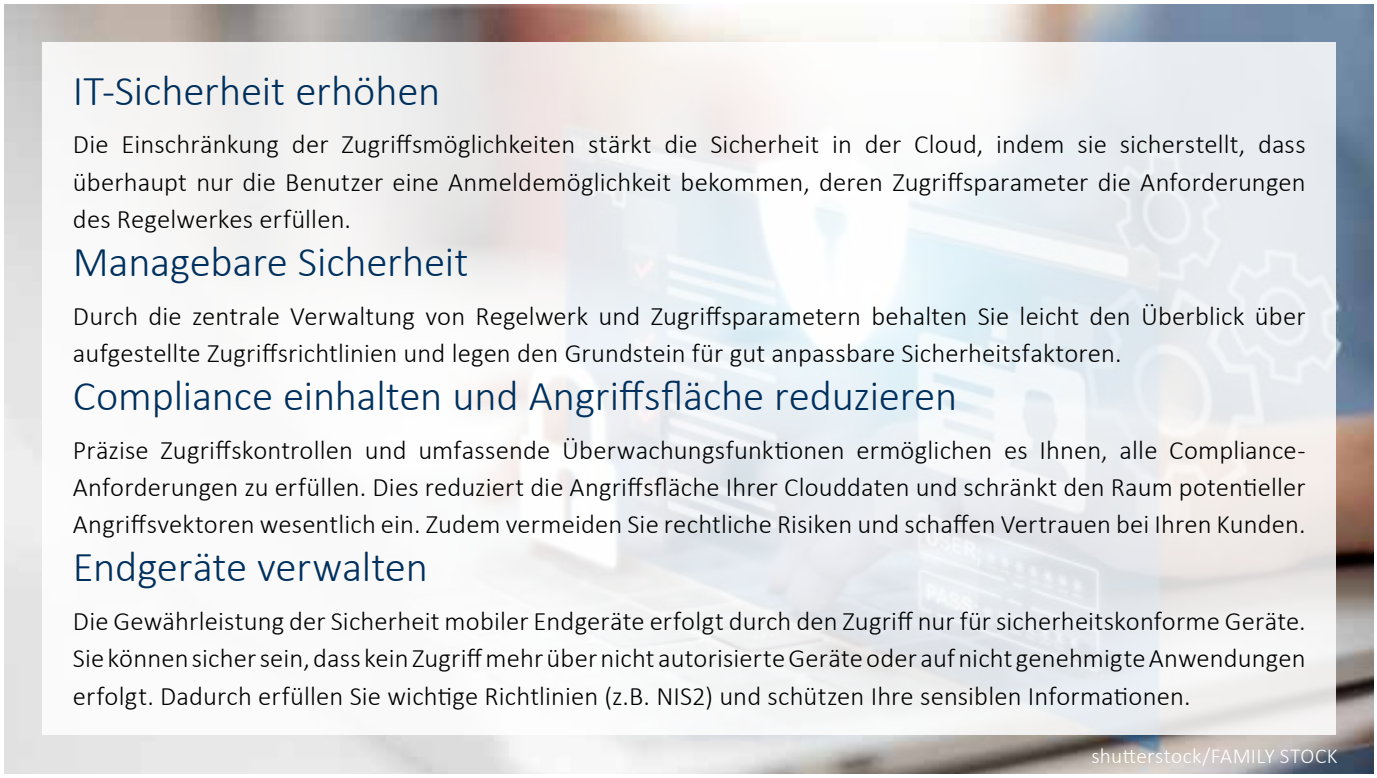
Optionale Folge-Dienstleistungen

Regelwerksaktualisierung:
Laufende Aktualisierung des Regelwerks gemäß Best Practices und neuen Funktionen für optimale Sicherheit.

MDM-Einführung:
Implementierung eines Mobile Device Management (MDM) Systems zur Sicherung und Standardisierung Ihrer Geräte.

Erweiterte Entra ID-Analyse:
Ausweitung der Analyse auf zusätzliche Aspekte von Entra ID zur Verbesserung der Sicherheitsrichtlinien.

Admin-Konzept & Kontoschutz:
Einführung eines umfassenden Admin-Konzepts zur Absicherung von Konten und Gewährleistung einer sicheren Benutzerverwaltung.



IT-Sicherheit erhöhen

Die Einschränkung der Zugriffsmöglichkeiten stärkt die Sicherheit in der Cloud, indem sie sicherstellt, dass überhaupt nur die Benutzer eine Anmeldemöglichkeit bekommen, deren Zugriffsparameter die Anforderungen des Regelwerkes erfüllen.

Managebare Sicherheit

Durch die zentrale Verwaltung von Regelwerk und Zugriffsparametern behalten Sie leicht den Überblick über aufgestellte Zugriffsrichtlinien und legen den Grundstein für gut anpassbare Sicherheitsfaktoren.

Compliance einhalten und Angriffsfläche reduzieren

Präzise Zugriffskontrollen und umfassende Überwachungsfunktionen ermöglichen es Ihnen, alle Compliance-Anforderungen zu erfüllen. Dies reduziert die Angriffsfläche Ihrer Clouddaten und schränkt den Raum potentieller Angriffsvektoren wesentlich ein. Zudem vermeiden Sie rechtliche Risiken und schaffen Vertrauen bei Ihren Kunden.

Endgeräte verwalten

Die Gewährleistung der Sicherheit mobiler Endgeräte erfolgt durch den Zugriff nur für sicherheitskonforme Geräte. Sie können sicher sein, dass kein Zugriff mehr über nicht autorisierte Geräte oder auf nicht genehmigte Anwendungen erfolgt. Dadurch erfüllen Sie wichtige Richtlinien (z.B. NIS2) und schützen Ihre sensiblen Informationen.

shutterstock/FAMILY STOCK

Kontaktieren Sie uns, um mehr über unser Angebot zu erfahren und einen individuellen Termin für die Analyse zu vereinbaren. Nutzen Sie die Gelegenheit, Ihre Cloud-Sicherheit auf das nächste Level zu heben!

Kontakt

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

BLUE CONSULT.