Day & Zimmerman

Eine Fallstudie wie der Bundesunternehmer Duo MFA verwendet, um den Fernzugriff seiner Mitarbeiter zu sichern und regulatorische Datenvorschriften einzuhalten.

Day & Zimmermann (D&Z) ist spezialisiert auf Bau-, Ingenieur-, Personal- und Verteidigungslösungen für Staatliche Behörden und führende Unternehmen weltweit. Mit 43.000 Mitarbeitern ist D&Z an mehr als 150 Standorten tätig und erzielt einen Umsatz von über 2,5 Milliarden US-Dollar. D&Z wird derzeit von Forbes als eines der größten privaten Unternehmen in den USA eingestuft.

Seit 2014 setzt D&Z Duo erfolgreich ein. Duo wurde ursprünglich zur Sicherung des Remotezugriffs von Benutzern über Cisco VPN eingesetzt und schützt jetzt seitdem mehere Systeme von D&Z, einschließend Outlook Web Access-, Citrix XenApp-, Thycotic-, Passwordstate- und Windows-Servern über Remote Desktop Protocol (RDP).

Die Herausforderung

Die geschäftlichen Herausforderungen

Als Auftragnehmer des US-Verteidigungsministeriums (DoD) muss D&Z die Vorschriften für kontrollierte nicht klassifizierte Informationen (Controlled Unclassified Information, CUI) einhalten. Bei Nichteinhaltung würden alle Regierungsverträge von D&Z gekündigt werden, was dazu führt das Millionen von Dollar dem Unternehmen verloren gehen.

D&Z haben rund 1.500 Mitarbeiter die aus mehreren Kundenstandorten auf der ganzen Welt arbeiten. Die besondere Herausforderung besteht darin den Mitarbeitern einen sicheren Zugriff auf die Systeme zu ermöglichen mit denen sie arbeiten und gleichzeitig die bestehenden Vorschriften einzuhalten.

Die Technische Herausforderungen

Die Mitarbeiter, die an Verträgen der US-Regierung arbeiten, müssen laut Verordnung beim Zugriff auf CUI eine 2-Faktor Authentifizierung (2FA) durchführen. Da CUI möglicherweise auf dem Computer des Endbenutzers vorhanden ist, besteht die einzige Möglichkeit, diese Anforderung zu erfüllen darin, beim Anmelden und Entsperren 2FA durchzuführen. Dadurch wird sichergestellt das der Computer des Endbenutzers auf die CUI zugreift und die auf diesem Computer installierten Anwendungen sicher ausführt, oder als sichere Auffahrt zum Rest des Netzwerks fungiert.

Diese Bestimmungen sind im DFARS (Defense Federal Acquisition Regulation Supplement) 252.204-7012 und im NIST SP 800-171 definiert, die eine „Multi-Faktor Authentifizierung für den lokalen und Netzwerkzugriff auf privilegierte Konten“ vorschreiben. Diese Regeln gelten für alle Organisationen die CUI verarbeiten, speichern oder übertragen.

D&Z Angestellte können sich jedoch nicht immer auf die Internetverfügbarkeit verlassen, um eine 2FA abzuschließen. Sie sind möglicherweise vorübergehend offline (z. B. auf einem Flug) oder können WLAN beim Kunden nicht nutzen. “Es ist auch schwierig, Benutzer beim Einstieg in ein neues, bisher unbekanntes WLAN-Netzwerk in einem fernen Land zu unterstützen, um ihre 2-Faktor Authentifizierung abzuschließen”, sagt Honer.

Für D&Z ist es auch wichtig, eine durchgängige Benutzererfahrung bereitzustellen, unabhängig davon, ob der Benutzer online oder offline ist, im Büro, von zu Hause oder an einem Remote-Kunden-Standort arbeitet. Andernfalls würde dies zu Verwirrung unter den Benutzern führen sowohl als zu höheren Supportkosten für das Unternehmen bedeuten.

Unsere Lösung

Zur Unterstützung seiner reisenden und Fern-Mitarbeiter nutzt D&Z die Offline-Authentifizierungsfunktionen von Duo. Honer gefällt besonders die Tatsache, dass die Benutzererfahrung genau gleich ist, unabhängig davon ob ein Benutzer online oder offline ist. Mit dieser Funktion können D&Z Benutzer nahtlos zwischen Online- und Offline-Umgebungen wechseln.

„Die ideale Situation ist ein Produkt, das sowohl den Online- als auch in den Offline-Modus für den Benutzer transparent unterstützt. Duo bietet dies allen unseren Angestellten”, laut Honer.

> “Duo is the most successful end-user facing solution I’ve ever been involved in deploying.”

Lance Honer
Manager of Cybersecurity

> **“Duo is the partner we rely on in our journey towards a zero-trust model.”**

Andrew Spenceley
Cyber Security Architect, University of Sunderland

> **“Duo Beyond has enabled us to push our zero-trust strategy faster.”**

Mike Johnson
CISO, Lyft

Starten Sie Ihre kosstenlose 30-Tage-Testversion und beschützen Sie alle Ihre benutzer, Geräte und Anwendugen auf **duo.com**.

Duo Security

Duo ist eine Cloud-basierte Sicherheitsplattform, die den Zugriff auf alle Anwendungen für jeden Benutzer und jedes Gerät von überall aus schutzt. Es ist so konzipiert, dass es sowohl einfach zu verwenden als auch bereitzustellen ist und gleichzeitig vollständige Sichtbarkeit und Kontrolle des Endpunkts bietet.

Duo überprüft die Identität der Benutzer mit einer starken Multi-Faktor Authentifizierung. Zusammen mit umfassenden Einblicken in die Geräte Ihrer Benutzer bietet Duo Ihnen die Richtlinien und die Kontrolle, die Sie benötigen, um den Zugriff basierend auf dem Endpunkt- oder Benutzerrisiko zu beschränken. Benutzer erhalten mit das Single Sign-On von Duo eine konsistente Anmeldeerfahrung, die einen zentralen Zugriff auf lokale und Cloud-Anwendungen ermöglicht.

Mit Duo können Sie sich vor gefährdeten Anmeldeinformationen und riskanten Geräten sowie vor unerwünschtem Zugriff auf Ihre Anwendungen und Daten schützen. Diese Kombination aus Benutzer- und Gerätevertrauen bildet eine solide Grundlage für ein Zero-Trust Sicherheitsmodell.