

Mehr Sicherheit, weniger Komplexität: Zehnders Weg zu Zero Trust



“

ZTNA ermöglicht uns eine deutlich präzisere und sicherere Zugriffskontrolle als unser früheres VPN.

Jörg Allemann, IT Director (CIO)

”

Überblick

Die Zehnder Group mit Sitz in Gränichen (Schweiz) entwickelt und produziert seit über 125 Jahren Lösungen für ein energieeffizientes und gesundes Raumklima. Um Sicherheit, Transparenz und Benutzerfreundlichkeit zu verbessern, modernisierte das Unternehmen seinen Remote Access mit ZTNA und CSWG von Open Systems. Die neue Lösung ermöglicht granulare Zugriffskontrollen, unterstützt hybride Arbeitsmodelle und bildet einen wichtigen Baustein der Zero-Trust-Strategie von Zehnder.

Kundendetails

- | | |
|---|--|
|  Produktions-gewerbe |  Gränichen, Schweiz |
|  70 Länder |  4,000 |
|  zehndergroup.com | |

Eingesetzte Produkte

- ZTNA & CSWG
- SD-WAN

Die Ergebnisse

-  **>1.500 Nutzer**
über ZTNA
-  **ZTNA & CSWG**
global eingeführt
-  **Verbesserte Sicherheit**
durch reduzierte Angriffsfläche
-  **Granulare Zugriffskontrolle**
für alle Nutzergruppen
-  **Reduzierte Komplexität**
durch Ablösung klassischer VPN-Strukturen
-  **Globaler Zugriff**
auf Unternehmensressourcen

Interview

Wir sprachen mit **Jörg Allemann** und **Willem de Groot** über IT-Herausforderungen und -Zielsetzungen bei Zehnder – und darüber, wie Open Systems eine ganzheitliche Lösung ermöglicht hat.

Was ist eure Rolle bei Zehnder und welche Verantwortung trägt ihr speziell bei Gestaltung und Schutz des Netzwerkzugriffs?

Jörg Allemann

Als Chief Information Officer der Zehnder Group trage ich die Gesamtverantwortung für die IT. Aufgrund unserer internationalen Aufstellung mit Standorten in Europa, Nordamerika und Asien – insbesondere in China – spielt das Netzwerk eine zentrale Rolle. Entsprechend hat die sichere und zuverlässige Vernetzung für mich eine sehr hohe Priorität.

Willem de Groot

Ich bin für die operative Umsetzung verantwortlich und wirke aktiv an der Gestaltung der Architektur mit. Dazu gehören sowohl Designentscheidungen als auch die Auswahl und Weiterentwicklung der eingesetzten Lösungen.

“

Der Managed Service von Open Systems entlastet uns deutlich und sorgt gleichzeitig für einen stabilen Betrieb.

Willem de Groot, Senior Network System Engineer

”

Was war der Auslöser, eure bisherige Sicherheitsarchitektur zu verändern?

Das Thema Sicherheit hat bei uns grundsätzlich einen sehr hohen Stellenwert, da unsere Supply Chain geschäftskritisch ist. Wir liefern physische Produkte, die zur richtigen Zeit am richtigen Ort beim Kunden ankommen müssen. Dafür sind stabile, sichere und jederzeit verfügbare Systeme und Prozesse unerlässlich. Entsprechend wichtig ist es für uns, sowohl die Konnektivität zuverlässig sicherzustellen als auch den Zugriff gezielt zu steuern.

Zusätzlich betreiben wir Produktionsstandorte und arbeiten mit externen Partnern zusammen, die ebenfalls sicheren Zugriff auf unsere Systeme benötigen. Gleichzeitig standen wir vor der Herausforderung, dass einzelne Komponenten das Ende ihres Lebenszyklus erreicht hatten und ersetzt werden mussten.

Ein weiterer wichtiger Aspekt war unser Anspruch, die Architektur insgesamt zu vereinfachen. Wir sind überzeugt, dass weniger Komplexität die Grundlage für mehr Sicherheit und bessere Steuerbarkeit bildet. Parallel dazu hat sich auch die Bedrohungslage im Internet deutlich verschärft – Risiken nehmen zu, und entsprechend steigt der Bedarf an leistungsfähigen Schutzmechanismen.

Welche konkrete Herausforderung hat dazu geführt, dass ihr euch für ZTNA und CSWG entschieden habt?

Wir haben erkannt, dass unser bisheriger Remote Access nicht mehr dem aktuellen Stand der Technik entsprach. Insbesondere die klassische VPN-Lösung mit Full-Tunnel-Ansatz war für unsere Anforderungen nicht mehr geeignet.

Gleichzeitig haben sich die Arbeitsweisen stark verändert: Remote Work hat deutlich zugenommen, wodurch auch die Anforderungen an sichere und skalierbare Zugriffslösungen gestiegen sind.



Unsere bestehende Infrastruktur basierte auf wenigen zentralen Zugangspunkten, was in einem globalen Umfeld klare Nachteile mit sich brachte.

Mit der neuen Lösung verfügen wir nun über deutlich bessere Möglichkeiten zur granularen Steuerung von Zugriffen. Das ist ein zentraler Baustein unserer Zero-Trust-Strategie, die wir schrittweise umsetzen. Die Lösung von Open Systems ist für uns dabei ein wichtiger Enabler.

Ein weiterer entscheidender Faktor war unsere Teamgröße. Für uns war ein Managed-Service-Ansatz deutlich sinnvoller, als verschiedene Komponenten selbst zu betreiben und zu integrieren. Zudem war es uns wichtig, eine integrierte Lösung aus einer Hand zu erhalten und nicht mehrere Anbieter koordinieren zu müssen.

Warum habt ihr euch speziell für Open Systems entschieden?

Wir haben verschiedene Alternativen geprüft und dabei die üblichen Kriterien zugrunde gelegt. Die Lösung musste architektonisch zu unserer bestehenden Umgebung passen – was insbesondere durch die bereits vorhandene SD-WAN-Infrastruktur von Open Systems gegeben war. Auch der Managed-Service-Ansatz war für uns ein wesentliches Entscheidungskriterium.

Neben den technischen Aspekten spielte selbstverständlich auch die Wirtschaftlichkeit eine wichtige Rolle. Die Lösung musste sich im Gesamtbild rechnen. In der Kombination aus Funktionalität, Integration und Kosten hat Open Systems uns überzeugt. Unsere Entscheidung basierte daher nicht nur auf der bestehenden Zusammenarbeit, sondern auf einer fundierten Gesamtbewertung.



“

Die Transparenz hat sich deutlich verbessert. Über das Open Systems Portal sehen wir, wer wann worauf zugreift.

Jörg Allemann, IT Director (CIO)

”

Wie verlief die Konzeptions- und Implementierungsphase der ZTNA- und CSWG-Lösungen in eurer Organisation?

Der Projektstart hat etwas Zeit in Anspruch genommen, da auf unserer Seite parallel weitere Initiativen liefen. Mit Unterstützung unserer Technical Account Manager bei Open Systems konnten wir das Projekt jedoch strukturiert vorantreiben.

Auch die Integration in bestehende Systeme verlief problemlos. Es gibt nur vereinzelt Fälle, in denen Zugriffsrechte nachträglich angepasst werden müssen – was bei einem solchen Projekt jedoch zu erwarten ist. Insgesamt läuft das System stabil und zuverlässig.

In einer ersten Phase haben wir die grundlegende Konnektivität aufgebaut und ZTNA erfolgreich eingeführt. Aktuell befinden wir uns in der nächsten Phase, in der wir die Zugriffskontrollen weiter verfeinern und noch granularer gestalten.

Zum einen sollte die Deadline eingehalten werden, zum anderen aber nicht der laufende Betrieb unterbrochen. Wie lief das für euch?

Die Migration konnten wir ohne Unterbrechung des laufenden Betriebs umsetzen. Wir hatten zwar ein Migrationswochenende, an dem es aber wie geplant keinerlei Ausfälle gab. Da wir teilweise auch am Wochenende produzieren, war ein durchgängiger Zugriff zwingend erforderlich.

Aufgrund vertraglicher Vorgaben mit unserem vorherigen Anbieter hatten wir eine feste Deadline. Der Zeitplan war ambitioniert, konnte aber durch eine enge Zusammenarbeit mit Open Systems erfolgreich eingehalten werden.

Ein grosser Vorteil war unser Vorgehen ohne „Big Bang“. Stattdessen haben wir das neue System schon parallel zur vorherigen Lösung aufgebaut und die Nutzer schrittweise migriert. Dadurch konnten wir zur Deadline einen reibungslosen, fließenden Übergang sicherstellen.



Wie hat euch das Team von Open Systems während des Projekts unterstützt?

Die Unterstützung war durchweg sehr gut. Trotz eines teilweise hohen Drucks – insbesondere durch parallele interne Projekte – verlief die Zusammenarbeit effizient und strukturiert.

Die Aufgabenverteilung hat gut funktioniert: Open Systems hat vorbereitet, wir haben zugearbeitet, und darauf aufbauend wurden die nächsten Schritte umgesetzt. Insgesamt ist das Projekt wie erwartet verlaufen, und wir sind mit dem Ergebnis sehr zufrieden.

Auch unsere bisherigen positiven Erfahrungen mit Open Systems haben sich bestätigt – die Qualität der Zusammenarbeit ist konstant hoch.

Welche Verbesserung konntet ihr seit der Einführung feststellen?

Die Nutzerakzeptanz ist sehr hoch. Das Feedback ist durchweg positiv, insbesondere hinsichtlich Performance und Benutzerfreundlichkeit. Viele Anwender empfinden die neue Lösung als schneller und einfacher als die vorherige.

Darüber hinaus hat sich die Effizienz erhöht, und wir gehen davon aus, dass der Supportaufwand im Bereich Remote Access zurückgegangen ist.

Ein wesentlicher Fortschritt liegt im Bereich Sicherheit – auch wenn dieser für die Nutzer weniger sichtbar ist. Durch die granularen Zugriffskontrollen können Anwender nur noch auf die Ressourcen zugreifen, die sie tatsächlich benötigen. Gleichzeitig wird verhindert, dass Sicherheitsmechanismen umgangen werden, wie es bei klassischen VPN-Lösungen möglich war. Auch der externe Zugriff ist heute deutlich besser abgesichert.

“

In der Kombination aus Funktionalität, Integration und Kosten hat Open Systems uns überzeugt.

Jörg Allemann, IT Director (CIO)

”

Wie hat sich die Transparenz und Kontrolle über Nutzerzugriffe verändert?

Die Transparenz hat sich deutlich verbessert. Über das Open Systems Portal können wir nachvollziehen, welcher Nutzer wann auf welche Ressourcen zugreift – eine Möglichkeit, die wir zuvor nicht hatten.

Im Alltag steht diese Funktion nicht im Vordergrund, ist aber im Falle von Problemen äusserst hilfreich. Sie ermöglicht es uns, gezielt zu analysieren, was passiert ist. Diese zusätzliche Transparenz stellt für uns einen klaren Mehrwert dar.

Welche Auswirkung hatte die Lösung auf Remote-Work für euch?

Die Lösung unterstützt unsere Remote- und Hybridarbeitsmodelle sehr gut. Die Verbindungen sind stabil, und die Nutzer berichten von einer insgesamt deutlich verbesserten Erfahrung.

Ein weiterer Vorteil sind die weltweit verfügbaren Zugangspunkte. Dadurch entfallen unnötige Umwege, was sich positiv auf die wahrgenommene Performance auswirkt.

Welchen Rat würdet ihr anderen Unternehmen geben, die mit ähnlichen Herausforderungen beim sicheren Zugriff oder Netzwerkschutz zu kämpfen haben?

Netzwerk und Remote Access sind zentrale Services bezüglich Security und Usability und sollten entsprechend behandelt werden. Die zunehmende Vernetzung und Mobilität machen es notwendig, sich aktiv mit diesen Themen auseinanderzusetzen.

Es gibt verschiedene Lösungsansätze, und jedes Unternehmen sollte den für sich passenden Weg wählen – abhängig von Architektur, Anforderungen und Teamgrösse. Für uns hat sich ein Managed-Service-Ansatz als sinnvoll erwiesen, auch unter wirtschaftlichen Gesichtspunkten.

Wir empfehlen, mit einer kleineren Nutzergruppe zu starten und die Lösung schrittweise auszurollen, anstatt alles gleichzeitig umzustellen. Für uns war es entscheidend, zunächst die Konnektivität sicherzustellen, um das vorherige System ablösen zu können.

Wichtig ist ausserdem, ausreichend Zeit für die Umsetzung und Feinjustierung einzuplanen. Insbesondere die Einführung granularer Zugriffskonzepte ist ein fortlaufender Prozess.

“

Die Nutzer empfinden die neue Lösung als schneller, einfacher und komfortabler als die vorherige.

Willem de Groot, Senior Network System Engineer

”

Möchtet ihr sonst noch etwas über die Zusammenarbeit mit Open Systems teilen?

Mit Open Systems haben wir einen verlässlichen Partner, insbesondere da wir bereits zuvor im Bereich SD-WAN zusammengearbeitet haben. Dadurch konnten wir auf bestehenden Strukturen und Erfahrungen aufbauen.

Auch das Team, die Arbeitsweise und etablierte Betriebsmodelle wie Mission Control waren uns bereits vertraut. Das hat die Umsetzung des Projekts zusätzlich erleichtert und dazu beigetragen, dass wir die Lösung effizient einführen konnten.



Jörg Allemann
IT Director (CIO)
Zehnder Group



Willem de Groot
Senior Network System Engineer
Zehnder Group

Auf einen Blick

Die Herausforderung

Die bestehende Remote-Access-Lösung konnte die Anforderungen einer globalen Organisation mit zunehmend hybriden Arbeitsmodellen nicht mehr optimal erfüllen.

Gleichzeitig sollte die Sicherheit erhöht, die Komplexität reduziert und die Grundlage für eine Zero-Trust-Strategie geschaffen werden. Dazu stand die Ablösung von Systemen an, die das Ende ihres Lebenszyklus erreicht hatten.



Die Lösung

Zehnder führte ZTNA und CSWG von Open Systems ein.

Die neue Lösung ersetzt den klassischen VPN-Ansatz, ermöglicht granulare Zugriffskontrollen und unterstützt eine Zero-Trust-Strategie. Der Managed-Service-Ansatz reduziert Komplexität und entlastet die interne IT.



Die Ergebnisse

ZTNA und CSWG von Open Systems sorgen für höhere Sicherheit, bessere Performance und eine deutlich verbesserte User Experience. Zugriffe sind heute granular steuerbar und die Transparenz über Nutzeraktivitäten ist signifikant gestiegen. Gleichzeitig wurde die Komplexität reduziert und der Remote Access modernisiert.



Über Zehnder Group

Die Zehnder Group ist ein weltweit führender Anbieter von Lösungen für ein energieeffizientes, gesundes und komfortables Raumklima. Das Unternehmen beschäftigt rund 4.000 Mitarbeitende und ist in über 70 Ländern aktiv. Seit über 125 Jahren entwickelt und produziert Zehnder Raumwärmer, Heiz- und Kühldecken sowie Lüftungssysteme.