CYBERSECURITY ZWISCHEN HOMEOFFICE UND CAYMAN ISLANDS IN DER FINANZBRANCHE

> **Open Systems ermöglicht uns, weltweit sicher in derselben Cloud-Umgebung zu arbeiten – schnell, stabil und ohne Kompromisse.**
>
> **Chief Operating Officer,** Finanzdienstleister

ÜBERBLICK

Das international aufgestellte Finanzunternehmen stand vor steigenden Cyberrisiken, wachsenden Compliance-Anforderungen und begrenzten internen IT-Ressourcen.

Mit Open Systems setzte es auf eine ganzheitliche Sicherheitsarchitektur aus **ZTNA**, **Cloud Proxy** und **24x7 Managed Services**. Das Ergebnis: höhere Sicherheit, stabile Zugriffe weltweit, vereinfachtes Management, bessere Compliance-Nachweise und deutlich reduzierte Sicherheitsvorfälle – bei planbaren Kosten.

KUNDENDETAILS

- Finanzdienstleister
- 3 Kontinente
- ~40

EINGESETZTE PRODUKTE

- SD-WAN
- ZTNA

ERGEBNISSE

100 %
MALWARE-ABWEHR
in bekannten Fällen

24x7
SUPPORT
für reduzierten Personalbedarf

100 %
PLANBARKEIT
dank All-Inclusive-Flat-Pricing

0
SICHERHEITSVORFÄLLE
trotz hoher Angriffslage

100 %
CLOUD-FIRST-SECURITY
für sichere Remote-Arbeit

Wir sprachen mit dem Chief Operating Officer eines Schweizer Finanzdienstleisters über IT-Herausforderungen und -Zielsetzungen – und darüber, wie Open Systems eine ganzheitliche Lösung ermöglicht hat.

WAS IST IHRE ROLLE IM UNTERNEHMEN?

Ich bin Chief Operating Officer unserer Unternehmensgruppe. Obwohl wir insgesamt rund 40 Mitarbeitende beschäftigen, ist unsere Struktur international verteilt: Der Hauptsitz befindet sich in Zürich, wo ein kleines Kernteam von vier bis fünf Personen arbeitet. Die operativen Einheiten sind in Irland und Singapur angesiedelt, jeweils mit rund 16 Mitarbeitenden. Als Gruppen-COO verantworte ich insbesondere die gesamte IT-Infrastruktur und -Services, die wir unseren Standorten weltweit bereitstellen.

WELCHE HERAUSFORDERUNG WOLLTEN SIE GEMEINSAM MIT OPEN SYSTEMS ANGEHEN?

Die Zusammenarbeit mit Open Systems begann bereits, bevor ich zum Unternehmen stiess. Damals betrieben wir zusätzlich ein Büro in den USA, und das zentrale Ziel war, unsere verschiedenen Standorte zuverlässig miteinander zu vernetzen. Diese Verbindung unserer lokalen Server funktionierte von Anfang an sehr gut – und tut es bis heute.

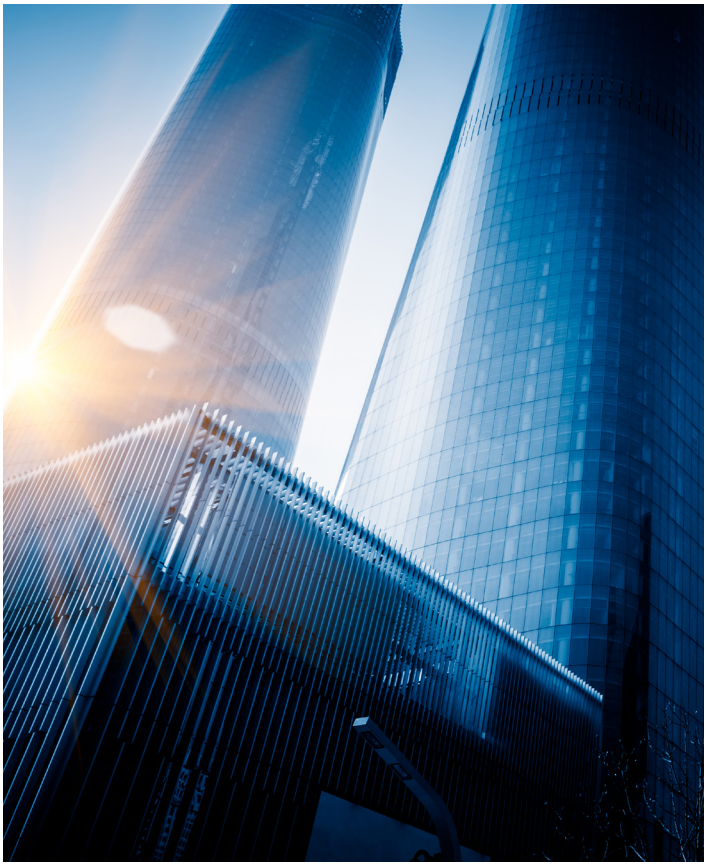
Mit dem Wechsel in die Cloud wurde diese Aufgabe noch bedeutender. Open Systems stellt nun sicher, dass alle Mitarbeitenden weltweit auf unsere Cloud-Umgebung zugreifen können – und das auf eine durchgängig sichere und stabile Weise.

WIE SAH IHRE NETZWERK- UND SECURITY-INFRASTRUKTUR AUS, BEVOR SIE MIT OPEN SYSTEMS ZUSAMMENGEARBEITET HABEN?

Früher beschäftigten wir zwei interne IT-Mitarbeitende, die sämtliche Aufgaben selbst abdeckten. Als ich ins Unternehmen kam, war nur noch eine Person für die interne IT zuständig. Als sie das Unternehmen verlassen hat, standen wir vor einer grundlegenden Entscheidung: eine neue interne Fachkraft einstellen oder die IT vollständig auslagern.

Wir entschieden uns für ein Outsourcing-Modell. Die interne IT-Infrastruktur übergaben wir an einen externen Cloud-Provider, während wir die Themen Firewall und Netzwerk in die Verantwortung von Open Systems legten. Meine Aufgabe besteht seither darin, die verschiedenen Dienstleister zu koordinieren.

Dieses Modell hat sich klar bewährt. IT muss heute rund um die Uhr verfügbar und geschützt sein. Gerade weil viele Cyberangriffe nachts oder am Wochenende stattfinden, war ein 24x7-Support für uns essenziell – und mit zwei oder drei internen Mitarbeitenden ist das schlicht nicht realisierbar. Deshalb halte ich Outsourcing in diesen Bereichen für den richtigen Weg, und Open Systems ist für uns dafür ein idealer Partner.



WIE HAT DIE NUTZUNG DES SD-WAN VON OPEN SYSTEMS IHREN ALLTAG VERÄNDERT?

Für ein Unternehmen unserer Grösse ist der Einsatz einer Proxy-Firewall eher ungewöhnlich. Sie macht das Setup zwar komplexer, erhöht aber die Sicherheit deutlich. Wir haben lange diskutiert, ob sich dieser Aufwand lohnt. Rückblickend kann ich klar sagen: Ja. In mindestens zwei Fällen hat uns die Proxy-Firewall davor geschützt, dass Malware eine Verbindung zu ihren Command-and-Control-Servern aufbauen konnte – genau dafür ist diese Lösung da.

Vor rund zwei Jahren haben wir dann eine grössere Umstellung vorgenommen. In Zürich arbeitet das Team etwa zur Hälfte im Homeoffice, und zuvor hatten wir hier noch eine physische Firewall. Heute setzen wir vollständig auf ZTNA und nutzen zusätzlich Cloud Proxys – eine Kombination, die sich für uns als äusserst effektiv erwiesen hat. Der Internetzugang erfolgt nun lokal über den Cloud Proxy, was in Zürich hervorragend funktioniert.

> **ZTNA hat unsere Sicherheit deutlich erhöht und gleichzeitig vieles vereinfacht. Der Zugriff ist präziser konfigurierbar und die Lösung ist wirklich ‚always on'.**

In Singapur und Irland betreiben wir weiterhin physische Firewalls im Büro, ergänzt durch ZTNA für das Arbeiten von zu Hause. Die gesamte Umstellung hat sich als sehr sinnvoll erwiesen und unsere Sicherheits- und Netzwerkinfrastruktur deutlich verbessert.

WARUM HABEN SIE VON MOBILE ENTRY POINT (MEP, CLIENT VPN) ZU ZTNA GEWECHSELT?

Vor der Umstellung verzeichneten wir zahlreiche Hacking-Versuche, und unsere User wurden immer wieder gesperrt – ein klarer Hinweis auf eine zu grosse Angriffsfläche. Gleichzeitig zeigte sich, dass der Betrieb mit unserem bisherigen Setup unnötig komplex war und ZTNA hier deutliche Vorteile bieten würde.

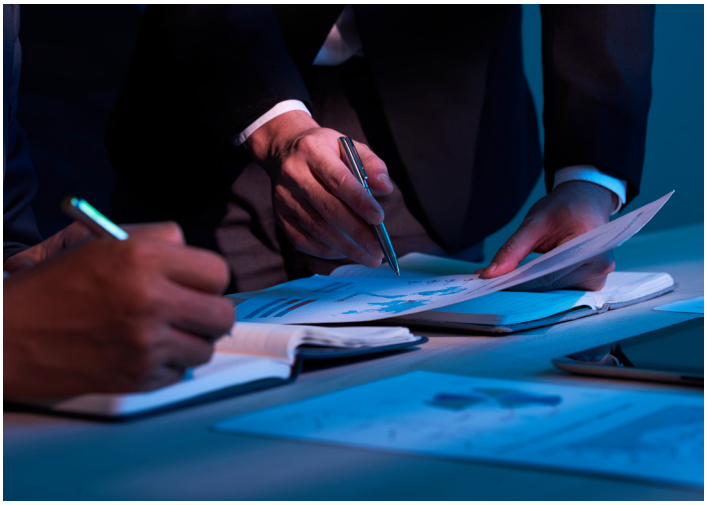
ZTNA erhöht nicht nur die Sicherheit, sondern reduziert auch die Abhängigkeiten von lokalen Komponenten. Beim Arbeiten von zu Hause benötigten wir zuvor MEP und meist einen lokal betriebenen Proxy, was teilweise zu Einschränkungen führte. Mit ZTNA in Kombination mit Cloud Proxys gewinnen wir deutlich mehr Flexibilität. Dank global verteilter Points of Presence ist der Einfluss auf die Performance erheblich geringer.

Besonders schätzen wir an ZTNA die feingranulare Zugriffskontrolle und die Möglichkeit, eine echte Always-on-Lösung bereitzustellen.

WARUM HABEN SIE SICH FÜR DAS ZTNA VON OPEN SYSTEMS ENTSCHIEDEN?

Wir waren bereits Open Systems Kunde und hatten durchweg sehr gute Erfahrungen gemacht. Zudem ist es für uns sinnvoll, alle sicherheitsrelevanten Services aus einer Hand zu beziehen – das vereinfacht die Zusammenarbeit deutlich. Auch das Preis-Leistungs-Verhältnis überzeugt uns.

Besonders schätzen wir die All-inclusive-Lösung: Durch das transparente Flat Pricing können wir unsere IT-Kosten verlässlich planen und behalten jederzeit die volle Übersicht.



GAB ES ANFORDERUNGEN AUS DER FINANZBRANCHE, DIE IHRE ENTSCHEIDUNG BEEINFLUSST HABEN?

Wir sind ein attraktives Ziel für Cyberangriffe – das zeigt sich an der grossen Zahl an Phishing-E-Mails, die wir täglich erhalten. Als Finanzunternehmen, das regelmässig hohe Transaktionssummen abwickelt, versuchen Angreifer insbesondere, Man-in-the-Middle-Attacken durchzuführen: Sie kompromittieren E-Mail-Konten unserer Kunden oder versuchen, sich Zugang zu unseren Systemen zu verschaffen, um anschliessend gefälschte Rechnungen mit manipulierten Kontodaten zu versenden. Solche Versuche erleben wir laufend, weshalb höchste Wachsamkeit erforderlich ist. Genau deshalb setzen wir auf die Sicherheitslösungen von Open Systems – sie helfen uns, diese Risiken konsequent zu reduzieren.

WELCHE ROLLE SPIELT DER 24X7 MANAGED SERVICE FÜR SIE IM TÄGLICHEN BETRIEB?

Das ist für uns ein zentraler Faktor: Wenn ein Sicherheitsvorfall auftritt – was erfahrungsgemäss häufig abends oder am Wochenende passiert – ist es enorm wertvoll, auf einen echten

24x7-Service zurückgreifen zu können. Auch unser Cloud Service Provider bietet Rund-um-die-Uhr-Support, und im Ernstfall greifen diese Services nahtlos ineinander. Dadurch wissen wir, dass wir im Notfall jederzeit schnell und zuverlässig unterstützt werden.

WELCHE KONKRETEN VERBESSERUNGEN HABEN SIE DURCH DIE ZUSAMMENARBEIT GESEHEN?

Ich kenne zwei konkrete Fälle, in denen unsere Proxy-Firewall verhindern konnte, dass Malware eine Verbindung zu einem Host aufbaut. Solche Risiken entstehen ständig, etwa wenn jemand unbeabsichtigt schädliche Dateien öffnet. In beiden Fällen schlug der Virenscanner Alarm und die Firewall blockierte die Verbindung zuverlässig. Solche Vorfälle passieren wahrscheinlich häufiger, als man denkt. Auch in den Log-Dateien sieht man regelmässig, welche Bedrohungen abgewehrt werden. Für uns zeigt das deutlich, wie wirksam diese Sicherheitsmassnahme ist.

WIE UNTERSTÜTZT ZTNA IHRE REGULATORISCHEN ANFORDERUNGEN (BAFIN, DSGVO, ISO 27001 USW.)?

ZTNA unterstützt uns wesentlich bei der Erfüllung von Compliance-Anforderungen und erleichtert uns damit das Ausfüllen zahlreicher Fragebögen. Unsere lokalen

Niederlassungen in Irland und auf den Cayman Islands unterliegen strengen regulatorischen Vorgaben, und auch viele unserer Kunden verlangen entsprechende Nachweise.

Ein weiterer wichtiger Punkt ist die Versicherung: Mittlerweile erhält man kaum noch eine Police, wenn man nicht nachweisen kann, dass umfangreich in Cybersecurity investiert wurde. Für uns war das nie ein akutes Problem, denn wir haben unsere Sicherheitsmassnahmen über die Jahre kontinuierlich ausgebaut. Diese Investitionen haben sich deutlich ausgezahlt.

WIE WÜRDEN SIE DIE USER EXPERIENCE HEUTE BESCHREIBEN IM VERGLEICH ZU FRÜHER?

Die User Experience und auch das Mission Control Portal werden immer besser. Die Implementierung von ZTNA erfordert zunächst einen erheblichen Aufwand, da die Konfiguration sehr präzise erfolgen muss. Genau dieser Aufwand erhöht jedoch die Sicherheit erheblich. Unser Technical Account Manager bei Open Systems ist dabei ein entscheidender Vorteil, da er unser Setup bestens kennt. Im Rahmen des Managed Service modernisieren wir es aktuell gemeinsam, sodass künftig Updates, etwa durch Änderungen seitens Microsoft, automatisch übernommen werden.

> **„ZTNA hilft uns enorm beim Erfüllen von Compliance-Anforderungen. Gerade für unsere Standorte in Irland und auf den Cayman Islands, wo viele regulatorische Fragebögen erforderlich sind."**

Dieser Ansatz erleichtert zudem das Management erheblich. Früher war es für die Mitarbeitenden oft kompliziert, wenn unterschiedliche Firewall-Regeln für Büro und Homeoffice galten. Durch die Vereinheitlichung des Zugriffs über ZTNA wird die Handhabung deutlich einfacher und benutzerfreundlicher.

WAS SCHÄTZEN SIE BESONDERS AN DER ZUSAMMENARBEIT MIT OPEN SYSTEMS?

Die Zusammenarbeit mit Open Systems ist stets sehr effizient. Wenn wir Unterstützung benötigen, erhalten wir schnell eine Lösung – auch in Notfällen, wenn es wirklich kritisch wird. Besonders schätze ich, dass technische Themen klar und verständlich erklärt werden. Das macht die Zusammenarbeit ausgesprochen angenehm, vor allem für mich als jemanden mit Finanz- statt IT-Hintergrund. So kann ich auch als Nicht-IT-Profi alle Abläufe problemlos gemeinsam mit den Open Systems-Mitarbeitenden steuern.

WELCHE NÄCHSTEN SCHRITTE PLANEN SIE IM BEREICH ZERO TRUST?

Bislang haben wir noch keine konkreten nächsten Schritte geplant. In den letzten zwei bis drei Jahren haben wir bereits sehr viel umgesetzt, und momentan liegt der Fokus auf der Konsolidierung. Danach werden wir prüfen, welche Massnahmen als Nächstes sinnvoll sind.

WO SEHEN SIE DEN NÄCHSTEN SCHRITT IN IHRER NETZWERK- ODER SICHERHEITSSTRATEGIE?

Derzeit beschäftigen wir uns mit CASB (Cloud Access Security Broker). Unsere Mitarbeitenden nutzen zunehmend Online-Tools, etwa PDF-Konverter, und genau solche Anwendungen möchten wir entweder blockieren oder zumindest besser kontrollieren. Ich erwarte, dass dieser Bedarf mit dem zunehmenden Einsatz von KI noch deutlich steigen wird.

> **Wir sind ein attraktives Ziel für Hacker, aber dank Open Systems haben wir unsere Sicherheitsbasis so stark ausgebaut, dass wir heute sehr gut geschützt sind.**

Ich selbst bin ein grosser Fan von KI und nutze sie intensiv, aber genau hier liegt die Herausforderung: KI-Anwendungen machen das System in vielerlei Hinsicht durchlässig. Während man versucht, Daten zu schützen, fliesen Informationen oft unkontrolliert ab, was problematisch ist.

Die ideale Lösung hierfür haben wir noch nicht gefunden. Vermutlich muss man sich bei einigen Anbietern auf deren Sicherheitsstandards verlassen – so wie viele Nutzer etwa bei Microsoft nach dem Motto „Was Microsoft macht, ist in Ordnung“. Bei Tools wie Perplexity in Kombination mit dem neuen Comet-Browser ist beispielsweise schwer nachzuvollziehen, welche Daten übertragen werden, wodurch die Kontrolle über sensible Informationen erschwert wird.

WAS WÜRDEN SIE ANDEREN UNTERNEHMEN RATEN, DIE VOR ÄHNLICHEN HERAUSFORDERUNGEN STEHEN?

Ich bin überzeugt, dass es sich auf jeden Fall lohnt, ausreichend in Cybersecurity zu investieren. Schon ein grösserer Zwischenfall kann für eine kleine oder mittelgrosse Firma ausreichen, um das Vertrauen der Kunden zu verlieren. Deshalb ist es sinnvoll, von Anfang an genug Ressourcen in die Sicherheit zu stecken, um solche Risiken zu minimieren.

GIBT ES NOCH EINEN ASPEKT DER ZUSAMMENARBEIT MIT OPEN SYSTEMS, DEN SIE BESONDERS HERVORHEBEN MÖCHTEN?

Besonders positiv hervorzuheben ist der 24x7 Managed Service, der rund um die Uhr einen Ansprechpartner bietet. Selbst am Wochenende werden Tickets bearbeitet, falls es ein Problem gibt. Gleichzeitig profitieren wir vom lokalen Bezug: Nicht nur die Produktentwicklung und das Account Management, sondern auch viele Support-Mitarbeitende sitzen in der Schweiz beziehungsweise arbeiten nach Schweizer Qualitäts-Standards, und die sind einfach sehr hoch.

AUF EINEN **BLICK**

DIE HERAUSFORDERUNG

International reguliert, stark im Fokus von Phishing und Betrugsversuchen und mit verteilten Standorten stand das Finanzunternehmen vor der Aufgabe, höchste Sicherheits- und Compliance-Anforderungen effizient und zuverlässig umzusetzen.

.

DIE LÖSUNG

Mit SD-WAN, ZTNA und Managed Services von Open Systems vereinheitlichte das Finanzunternehmen den sicheren Zugriff weltweit. 24x7-Support und reduzierte Komplexität sorgen für hohe Sicherheit bei einfacher Nutzung.

DIE ERGEBNISSE

- Deutlich **höhere Sicherheit** bei gleichzeitig **besserer User Experience**
- **Hohe Compliance- und Audit-Fähigkeit** trotz internationaler Regulierung
- **Weniger operativer IT-Aufwand** durch vereinheitlichte Zugriffe und Services
- **Verlässlicher 24x7-Betrieb** mit **planbaren Kosten** und schneller Unterstützung

Open Systems bietet co-managed SASE-Betriebsmodelle, die sichere Konnektivität, Zero-Trust-Modelle und transparenten 24×7 Betrieb für komplexe hybride und Multi-Cloud-Unternehmensumgebungen in mehr als 180 Ländern vereinen.