



## UBS stellt höchste Anforderungen an Zuverlässigkeit und Vertraulichkeit

### DIE HERAUSFORDERUNG

- Nachfolgelösung eines E-Mail-Filter-systems, das einen sehr hohen Maturitätsgrad erreicht hatte
- Zuverlässigkeit, Vertraulichkeit, Sicherheit und Compliance
- Aus regulatorischer Sicht eine Lösung aus der Schweiz gesucht
- Aufrechterhaltung der Produktivität in mehr als 55 Ländern

### DIE LÖSUNG

- Open Systems  
Secure Email Gateway
- 24x7-Betrieb und Security  
Monitoring von L3 Ingenieuren

### DAS RESULTAT

- Zuverlässige und stabile Services, die vom Prozessablauf her, bestens in den E-Mail-Betrieb von UBS integriert sind
- Kontinuierliche Weiterentwicklung und Verfeinerung der Filtermethoden
- Ein solider Partner, der das Geschäft versteht und über die Arbeitskultur verfügt, um einen Hochqualitätsjob zu machen

### Das Unternehmen

Die globale Bank mit starken Schweizer Wurzeln betreut seit über 150 Jahren private, institutionelle und Firmenkunden weltweit ebenso wie Retailkunden in der Schweiz. Strategisch positioniert sich der globale Finanzdienstleister mit einem herausragenden globalen Wealth Management sowie als führende Universalbank in der Schweiz. Gemeinsam mit einer kundenorientierten Investment Bank und einem starken, gut diversifizierten Global Asset Management, erweitert die UBS ihre erstklassige Marktstellung im Wealth Management und treibt das Wachstum im gesamten Konzern weiter voran.

### DIE HERAUSFORDERUNG

UBS hat den Arbeitsablauf mit dem Vorgängerfiltersystem für E-Mails über mehrere Jahre auf einen sehr hohen Maturitätsgrad gebracht. Als klar wurde, dass eine Nachfolgelösung gesucht werden musste, war wichtig, die Qualität für die User zu halten oder sogar zu verbessern. Zudem war für die Bank bezüglich Zuverlässigkeit, Vertraulichkeit sowie aus regulatorischer Sicht eine Lösung aus der Schweiz zwingend.

Die Mitarbeiterinnen und Mitarbeiter des global tätigen Finanzdienstleisters UBS erhielten in einem Durchschnittsmonat zusammengerechnet mehr als 130 Millionen E-Mails. Gut 70 Prozent davon, also über 90 Millionen E-Mails, waren Spam und deshalb unerwünscht. Es war nötig dafür zu sorgen, dass die Benutzer der IT-Infrastruktur des UBS-Konzerns in mehr als 55 Ländern produktiv arbeiten können und dabei die vom Konzern definierten technologischen Rahmenbedingungen einhalten.

Die UBS stellt höchste Anforderungen an Zuverlässigkeit und Vertraulichkeit. Das im globalen Business-Alltag zu erfüllen, ist in der IT eine anspruchsvolle Aufgabe.

## KUNDEN STORY

Die intellektuell geprägte Arbeitskultur in einem Finanzkonzern basiert auf Informationen, die heute praktisch nur noch digital zur Verfügung stehen. Ist der Zugriff auf diese Informationen nicht, nur teilweise oder zeitlich verzögert möglich, sind die Mitarbeiter in ihrer Handlungsfähigkeit massiv eingeschränkt.

Die regulatorischen Anforderungen sind sehr komplex und von Land zu Land unterschiedlich. Vereinfacht kann man jedoch sagen, dass die Regulatoren in den einzelnen Ländern den Auftrag haben zu überwachen, dass Tätigkeiten der Bank über mehrere Jahre hinweg dokumentiert und auditierbar sind. Auch das ist eine Auflage, die UBS mit der IT jederzeit sicherstellen muss.

Um der eigenen und die regulatorischen Auflagen zu erfüllen, sind die Datensysteme, auf denen Kundendaten liegen, in der Technologie-Welt der Bank strikte physisch und geographisch segregiert. Darauf Zugriff haben wirklich nur diejenigen Mitarbeiterinnen und Mitarbeiter, die entsprechende Berechtigungen haben.

### DIE LÖSUNG

#### Physische Abgrenzung in Zonen

Die Bank hat sich architektonisch so organisiert, dass sie in ihrem weltweiten Modell eine physische Abgrenzung in Zonen etabliert hat. Es wird unterschieden beispielsweise zwischen einer roten Zone und einer grünen Zone. In diesen Zonen hat man die höchstmöglichen Sicherheitsstandards etabliert.

#### Filter

Gefiltert wird vor der Lieferung der E-Mails in die Mailbox der Benutzer. Das ist eine zentrale Funktion, bei der alle nicht gewollten und zum Teil auch mit Virensignaturen befallenen E-Mail eliminiert und entsprechend ausgefiltert werden. Wir sprechen von über 70 Prozent Spam.

#### Datenpflege und Rechte

Die Pflege der E-Mail-Benutzerdaten passiert direkt über das zentrale Identity-Management-System, welches mit dem HR-System verknüpft ist. Darin ist auch festgehalten, wer im Konzern geographisch wo angesiedelt ist, welche Funktion ein Benutzer hat und welche Berechtigungen er oder sie für die Erledigung der Aufgabe braucht. So werden des Weiteren auch die Zugriffrechte auf IT-Systeme, Daten und Informationen geregelt.



“An Zuverlässigkeit und Vertraulichkeit stellen wir höchste Anforderungen.”

Markus Lickert, Managing Director  
and Head of End User Services, UBS

### DAS RESULTAT

Open Systems Services laufen sehr zuverlässig und stabil und sind vom Prozessablauf her bestens in den E-Mail-Betrieb integriert. UBS hat nach wie vor die volle Kontrolle über die Aktivitäten und kann im Bedarfsfall sehr rasch reagieren. Aus Sicht der Operations ist die 7x24-Betriebsorganisation von UBS in regem Austausch mit dem Open Systems Mission Control Center. Das wird als ein sehr gutes Zeichen gesehen.

Aus konzeptioneller Sicht verfügt UBS heute mit dem Secure Email Gateway über ein starkes Fundament. Es liegt aber in der Natur der Sache, dass die Weiterentwicklung eines solchen Services nie abgeschlossen sein kann. Das ist eine «never ending story». Gemeinsam mit den Security Engineers von Open Systems arbeitet das End User Services Team deshalb konstant daran, die Filtermethoden zu verfeinern und neue Prozesse und Mechanismen einzuführen, damit man die Erfolgsquote – und damit auch die User Experience – noch weiter verbessern kann. Auch in dieser Zusammenarbeit erleben UBS die Security Engineers von Open Systems als echte Partner, die sehr kompetent und offen sind, den bestehenden Service kontinuierlich zu optimieren.

#### Ein solider Partner

«Open Systems ist ein solider Partner, der das Geschäft fundiert versteht und beherrscht sowie über das Pflichtbewusstsein und die Arbeitskultur verfügt, um einen Hochqualitätsjob zu machen,» fasst Markus Lickert zusammen.



Open Systems ist Pionier im Bereich Secure Access Service Edge (SASE), der es Unternehmen ermöglicht, Netzverbindungen intern, zur Cloud und zum Rest der Welt herzustellen. Mit der Cloud-Architektur, dem Secure Service Edge, dem hybriden Cloud-Support, dem 7x24-Kontakt zu Level-3-Ingenieuren und der Predictive Analytics bietet SASE von Open Systems eine Komplettlösung für Netzwerke und IT-Sicherheit.