Wie ein Schweizer Asset Manager E-Mail-Risiken reduziert

Enabling Qapital

> **Wir konnten im Test klar sehen, dass bis zu 40 % mehr verdächtige E-Mails herausgefiltert werden – und genau das reduziert unser Risiko spürbar.**
>
> Christoph Dreher, Executive Management & Partner

Überblick

Enabling Qapital, ein FINMA-regulierter Schweizer Impact Asset Manager, stand vor der Herausforderung, gezielte Phishing-Angriffe erfolgreich abzuwehren, die trotz bestehender Schutzmaßnahmen E-Mail-Postfächer erreichten. Mit Advanced Email Security von Open Systems ergänzt das Unternehmen seine Sicherheitsarchitektur um eine vorgelagerte Schutzschicht. Ergebnis: bis zu 40 % mehr abgefangene E-Mails, deutlich geringeres Risiko und eine stärkere Absicherung des wichtigsten Angriffsvektors.

Kundendetails

- Financial Services
- Zürich, Schweiz
- 60
- enabling.ch

Eingesetzte Produkte

- Advanced Email Security
- Secure Email Gateway
- Advanced Threat Protection

Die Ergebnisse

- **Bis zu 40%** mehr abgefangene E-Mails
- **80-90%** der Angriffe effektiv adressiert (E-Mail als Hauptvektor)
- **Deutlich weniger riskante E-Mails** in der Inbox
- **Niedrige False-Positive-Rate** bei höherer Filterleistung
- **Zusätzlicher Sicherheits-Layer** vor der Inbox

Interview

Wir sprachen mit **Christoph Dreher**, Executive Management & Partner, über IT-Herausforderungen und -Zielsetzungen bei Enabling Qapital – und darüber, wie Open Systems eine ganzheitliche Lösung ermöglicht hat.

Was ist Ihre Rolle im Unternehmen und welche Verantwortung tragen Sie im Bereich IT-Security beziehungsweise E-Mail-Sicherheit?

Ich bin COO / CFO und verantworte somit in meiner Rolle unter anderem die Bereiche IT, HR und Finance. Bereits im zweiten Jahr nach der Gründung unseres Unternehmens haben wir entschieden, dass IT-Security auf Executive- beziehungsweise Board-Ebene verankert sein muss. Für uns hat Cybersecurity denselben Stellenwert wie Portfoliomanagement oder Business Development/Commercial.

Aufgrund unserer internationalen Präsenz bzw. Investments und der weit verteilten Mitarbeitenden ist IT-Sicherheit für uns ein geschäftskritischer Faktor. Es geht nicht nur darum, Angriffe abzuwehren, sondern vor allem um die potenziellen Auswirkungen eines Sicherheitsvorfalls.

Als Asset Manager leben wir vom Vertrauen unserer Kunden – und dieses Vertrauen muss sich auch in der Sicherheit unserer Systeme und Daten widerspiegeln.

Bereits in der Anfangsphase des Unternehmens wurde durch ein sicherheitsrelevantes Ereignis deutlich, wie wichtig robuste IT-Sicherheitsmassnahmen sind und welche Opportunitätskosten entstehen können, wenn entsprechende Vorkehrungen nicht konsequent priorisiert werden. Seitdem ist IT-Security fest auf oberster Ebene verankert und wird entsprechend priorisiert.

Trotz unserer vergleichsweise geringen Grösse – wir beschäftigen rund 60 Mitarbeitende und verwalten ein Vermögen von knapp unter einer Milliarde – sehen wir uns regelmässig Angriffen ausgesetzt, etwa durch Domain-Impersonation oder gezielte Phishing-Kampagnen. Das bestätigt unsere Überzeugung: Es gibt heute kein Unternehmen, das nicht betroffen ist.

Gleichzeitig ist IT-Security stark eine Frage des Mindsets. Da Massnahmen oft als grosser Kostenfaktor wahrgenommen werden und ihre Wirkung im Alltag kaum sichtbar ist, braucht es die klare Verankerung auf Geschäftsleitungsebene, um die notwendigen Investitionen nachhaltig durchzusetzen.

> **Bei uns kommen 80 bis 90 % der Angriffe über E-Mail – das ist ganz klar unser kritischster Angriffsvektor.**
>
> Christoph Dreher, Executive Management & Partner

Welche Bedeutung hat E-Mail-Sicherheit für Sie, auch im Kontext Ihrer globalen Aktivitäten?

E-Mail ist bei uns der zentrale Angriffsvektor. Unsere Endgeräte sichern wir durch ein umfassendes Device Management ab, doch in der Praxis zeigt sich, dass 80–90 % der Angriffe über E-Mail erfolgen. Der entscheidende Faktor ist dabei der Mensch: Letztlich liegt es immer am Nutzer, ob ein Angriff erfolgreich ist oder nicht.

Gerade im internationalen Kontext besteht ein erhöhtes Risiko, da unsere Kommunikationspartner weltweit tätig sind und nicht überall dieselben Sicherheitsstandards gelten. Auch deshalb betrachten wir eingehende E-Mails als das grösste Einfallstor für Bedrohungen.

Unser Ansatz ist zweistufig: Einerseits möchten wir möglichst viele Angriffe bereits vor Zustellung in die Inbox erkennen und blockieren. Andererseits investieren wir gezielt in Awareness-Trainings, um unsere Mitarbeitenden für potenzielle Risiken zu sensibilisieren. Für uns hat E-Mail-Sicherheit mindestens die gleiche Priorität wie das Device Management.

Welche konkreten Herausforderungen oder Risiken hatten Sie im Bereich E-Mail-Sicherheit vor der Zusammenarbeit mit Open Systems?

Ein prägender Einzelfall ereignete sich bereits ganz zu Beginn unserer Unternehmensgeschichte, kurz nach der Gründung und noch bevor wir gezielt in umfassendere IT-Security-Massnahmen investiert hatten. Damals wurde das E-Mail-Konto einer Mitarbeiterin kompromittiert und für Kommunikation missbraucht, ohne dass dies unmittelbar bemerkt wurde.

Dabei wurde versucht einen Geld-Transfer zu manipulieren. Darüber hinaus gab es Versuche, über E-Mails Schadsoftware einzuschleusen. Diese Erfahrungen haben uns gezeigt, wie E-Mail sowohl als direkter Angriffsvektor als auch als Instrument zur Ausweitung eines Angriffs genutzt werden kann.

Entsprechend verfolgen wir einen ganzheitlichen Ansatz: einerseits eine möglichst leistungsfähige E-Mail-Security, die Bedrohungen frühzeitig erkennt, und andererseits zusätzliche Schutzmechanismen wie Managed Detection and Response (MDR) sowie Managed Vulnerability Mitigation (MVM), um im Ernstfall schnell reagieren und betroffene Systeme isolieren zu können.

> **Im Asset Management leben wir von Vertrauen – und genau deshalb hat IT-Security für uns den gleichen Stellenwert wie Portfoliomanagement oder Business Development/Commercial.**
>
> Christoph Dreher, Executive Management & Partner

Welche Rolle spielen Ihre internationalen Standorte beziehungsweise Märkte für Ihre Security-Strategie?

Wir behandeln alle unsere Märkte grundsätzlich als gleichermassen risikobehaftet. Als vollständig cloud-basiertes Unternehmen – insbesondere mit Microsoft 365 – unterscheiden wir nicht zwischen einzelnen Regionen. Ob ein Mitarbeitender in der Schweiz oder in Nairobi arbeitet, spielt für unser Sicherheitsmodell keine Rolle.

Unser Ansatz basiert darauf, klare Trennungen zwischen internen und externen Systemen zu schaffen und Zugriffe konsequent zu kontrollieren. Perspektivisch streben wir eine Weiterentwicklung hin zu einem Zero-Trust-Ansatz an, bei dem grundsätzlich davon ausgegangen wird, dass jedes System potenziell kompromittiert sein kann und jeder Zugriff explizit autorisiert werden muss.

Was war der Auslöser für die Einführung von Advanced Email Security zusätzlich zur bestehenden Lösung?

Trotz bestehender Schutzmechanismen haben wir festgestellt, dass weiterhin relevante Bedrohungen durchkamen – insbesondere Angriffe, die beispielsweise als Nachrichten von DocuSign oder LinkedIn getarnt waren oder schadhafte Anhänge enthielten, wie PDFs und QR-Codes.

Ein zentrales Problem bei klassischen Lösungen ist, dass sie stark auf bekannte Muster und Datenbanken angewiesen sind. Neue, gezielte Angriffe werden dadurch oft nicht zuverlässig erkannt. Open Systems' Advanced Email Security bietet hier einen entscheidenden Mehrwert durch den Einsatz von Machine Learning und die Analyse von Kommunikationsbeziehungen.

Da ein grosser Teil unserer E-Mail-Kommunikation mit bekannten Partnern stattfindet, kann das neue System Abweichungen überdurchschnittlich schnell im Kommunikationsverhalten erkennen und entsprechend reagieren.

Die Kombination verschiedener Schutzansätze reduziert das Risiko deutlich, wie etwa KI-basierte Analysen von Anhängen, Links und QR-Codes sowie die Bewertung der Absenderreputation und typischer Kommunikationsmuster. Pro Nachricht werden zahlreiche Signale berücksichtigt und in den spezifischen Unternehmenskontext eingeordnet, um Auffälligkeiten frühzeitig zu identifizieren. Das zugrunde liegende System lernt dazu und passt sich dynamisch neuen Bedrohungsmustern an.

In der Testphase konnten wir feststellen, dass deutlich mehr potenziell gefährliche E-Mails erkannt und herausgefiltert wurden.

Warum haben Sie sich entschieden, diesen Schritt mit Open Systems zu gehen?

Neben der technischen Leistungsfähigkeit spielt für uns die Qualität der Zusammenarbeit eine zentrale Rolle. Wir legen grossen Wert auf verlässliche Partner und versuchen, die Komplexität im Vendor Management möglichst gering zu halten.

Der Service von Open Systems – insbesondere über Mission Control – überzeugt durch schnelle Reaktionszeiten und hohe fachliche Qualität. Anders als bei manchen Outsourcing-Modellen steht hier rund um die Uhr erfahrenes Personal zur Verfügung, das Entscheidungen fundiert und eigenständig treffen kann.

Hinzu kommen regulatorische Aspekte: Open Systems verfügt über ein sehr gutes Standing bei der FINMA sowie über relevante ISO- und SOC1/ISAE-Zertifizierungen. Auch der Standort in der Schweiz ist für uns als reguliertes Unternehmen ein wichtiger Faktor.

> **Der Service von Open Systems ist exzellent – schnell, kompetent und auf einem Niveau, das man so selten findet.**
>
> Christoph Dreher, Executive Management & Partner

Welche Rolle spielten Compliance-Anforderungen und Datensouveränität?

Compliance und regulatorische Anforderungen sind für uns zentral. Als reguliertes Unternehmen müssen wir sicherstellen, dass unsere IT-Sicherheitslösungen den Erwartungen von Aufsichtsbehörden und Auditoren entsprechen.

Die vorhandenen Zertifizierungen sowie die etablierte Position von Open Systems im Markt erleichtern sowohl Audits als auch die Abstimmung mit Regulatoren erheblich.

Auch das Thema Datensouveränität ist für uns relevant bzw. wurde im Rahmen der Risikoanalyse berücksichtigt. Als Microsoft-365-Kunde bewegen wir uns hier in einem gewissen Spannungsfeld (etwa im Kontext des CLOUD Act), setzen jedoch bewusst auf die erweiterten Customer Agreements von Microsoft für den Schweizer Finanzsektor (kurz auch «Swiss Cloud» genannt). Diese bietet die notwendigen Rahmenbedingungen, um regulatorische Anforderungen bestmöglich zu erfüllen und gleichzeitig die gewünschten Cloud-Vorteile zu nutzen.

Welche Erkenntnisse haben Sie aus dem Proof of Concept gewonnen?

Die Ergebnisse des Tests waren sehr positiv. Insbesondere fiel auf, dass viele E-Mails, die zuvor zumindest im Spam-Ordner gelandet wären, nun vollständig blockiert wurden, bevor sie den Benutzer erreichen konnten. Insgesamt konnten wir im Rahmen des Proof of Concept beobachten, dass rund 30-40 % mehr E-Mails herausgefiltert wurden als zuvor.

Gerade vor dem Hintergrund regelmässiger Phishing-Tests – sowohl automatisiert als auch manuell erstellt – wissen wir, wie häufig selbst geschulte Mitarbeitende auf täuschend echte Angriffe reagieren. Entsprechend entscheidend ist es, die Anzahl potenziell gefährlicher E-Mails in den Postfächern so gering wie möglich zu halten.

Advanced Email Security zeigte insbesondere bei der Analyse von Kommunikationsmustern und beim Erkennen komplexer Angriffstechniken – etwa via QR-Codes – klare Vorteile und filterte signifikant mehr Bedrohungen bei gleichzeitig niedriger False-Positive-Rate.

> **Viele sehen Email-Security als Kostenfaktor – bis etwas passiert und die wahren Kosten sichtbar werden.**
>
> Christoph Dreher, Executive Management & Partner

Welche messbaren Verbesserungen erwarten Sie?

Wir erwarten eine deutliche Erhöhung der Erkennungsrate bei Phishing-Angriffen, insbesondere bei gezielten und bislang unbekannten Angriffsmustern. Gleichzeitig ist es wichtig, dass die Anzahl der False Positives niedrig bleibt.

Ein wesentliches Ziel ist es, sichtbar zu machen, wie viele potenziell gefährliche E-Mails zusätzlich abgefangen werden und wie sich dieses Niveau im Zeitverlauf entwickelt. Diese Kennzahlen analysieren wir regelmässig.

Wie erleben Sie die Zusammenarbeit mit Open Systems?

Die Zusammenarbeit ist geprägt von Offenheit, direktem Austausch und hoher fachlicher Kompetenz. Trotz unserer Unternehmensgrösse haben wir feste Ansprechpartner, sowohl im Account Management als auch auf technischer Seite.

Im Vergleich zu anderen Anbietern erleben wir hier deutlich kürzere Reaktionszeiten und eine wesentlich höhere Qualität der Unterstützung. Das ist für uns ein entscheidender Mehrwert.

Insgesamt bewerten wir die Zusammenarbeit als durchweg ausgezeichnet.

Wie unterstützt Sie das Team konkret im Alltag?

Im operativen Alltag ist Mission Control unser zentraler Ansprechpartner. Dort werden Anfragen und Meldungen – beispielsweise zu False Positives – schnell und kompetent bearbeitet. Für uns ist dabei vor allem die Kombination aus Reaktionsgeschwindigkeit und fachlicher Qualität ausschlaggebend.

Warum würden Sie sich wieder für Open Systems entscheiden?

Ausschlaggebend sind für uns drei Faktoren: der exzellente Service, die hohe fachliche Kompetenz und die technologische Aktualität der Lösungen. Zudem überzeugt uns die klare Weiterentwicklungsstrategie und der Fokus auf relevante Sicherheitsthemen.

Welche Erkenntnisse haben Sie aus dem FINMA-Audit gewonnen – insbesondere im Hinblick auf Ihr Sicherheitsniveau im Vergleich zu anderen Unternehmen?

Für uns ist das Ergebnis des letzten IT-Audits ein klares Signal, dass wir mit unserer Sicherheitsstrategie auf dem richtigen Weg sind. Die Einordnung unter die Top 5 % zeigt, dass wir die relevanten Anforderungen nicht nur erfüllen, sondern in zentralen Bereichen ein überdurchschnittlich hohes Sicherheitsniveau erreichen. Gleichzeitig stärkt dies das Vertrauen unserer Kunden, dass ihre Daten bei uns bestmöglich geschützt sind. IT-Security ist damit ein integraler Bestandteil unseres Qualitäts- und Vertrauensversprechens.

Welchen Rat würden Sie anderen Unternehmen geben?

E-Mail-Sicherheit sollte als eines der zentralen Elemente der IT-Sicherheitsstrategie verstanden werden. Sie geht weit über klassischen Spam-Schutz hinaus und hat erheblichen Einfluss auf das Gesamtrisiko eines Unternehmens.

Unternehmen sollten bereit sein, in präventive Massnahmen zu investieren und sich nicht ausschliesslich auf Standardlösungen zu verlassen. Gerade vorgelagerte Schutzmechanismen, die E-Mails bereits vor Zustellung filtern, sind aus unserer Sicht essenziell.

Gleichzeitig zeigt unsere Erfahrung, dass auch etablierte Lösungen wie Microsoft 365 Defender nicht alle Angriffe zuverlässig erkennen. Ein mehrschichtiger Sicherheitsansatz, der unterschiedliche Technologien kombiniert, ist daher entscheidend, um das Risiko nachhaltig zu reduzieren.

Christoph Dreher
Executive Management & Partner
Enabling Qapital

Auf einen Blick

Die Herausforderung

Als international tätiges, in der Schweiz reguliertes Unternehmen ist Enabling Qapital einem konstant hohen Risiko durch Cyberangriffe ausgesetzt. Besonders E-Mail stellt das grösste Einfallstor dar, da viele Attacken gezielt auf Benutzerinteraktion abzielen. Trotz bestehender Schutzmassnahmen erreichten weiterhin raffinierte Phishing-Mails die Postfächer und erhöhten das Risiko für Manipulation, Datenverlust und finanzielle Schäden.

Die Lösung

Mit Advanced Email Security ergänzt Enabling Qapital seine bestehende Sicherheitsarchitektur um eine vorgelagerte Schutzebene. Durch heuristische Verfahren, KI-basierte Analyse und Kontextbewertung werden auch unbekannte Angriffsmuster identifiziert und blockiert – insbesondere bei gezielten Phishing-Mails.

Die Ergebnisse

Im Proof of Concept zeigte sich eine klare Verbesserung: Bis zu 40 % mehr potenziell gefährliche E-Mails wurden erkannt und abgefangen. Gleichzeitig gelangten deutlich weniger riskante Nachrichten in die Postfächer der Benutzer. Enabling Qapital profitiert von einer spürbar erhöhten Sicherheit entlang seines kritischsten Angriffsvektors bei weiterhin niedriger False-Positive-Rate.

Über Enabling Qapital

Enabling Qapital Ltd. (EQ) ist ein von der FINMA regulierter, führender Schweizer Impact Asset Manager, der sich für eine Welt einsetzt, in der Investitionen finanzielle, soziale, ökologische und wirtschaftliche Renditen erzielen. Mit über 900 Mio. USD verwaltetem Vermögen investiert EQ über Private Debt und börsennotierte Anleihen in Mikrofinanzierung, Energiezugang und Schwellenländeranleihen.

Open Systems ist ein KI-gestützter SASE-Plattformanbieter, der sichere Zugriffe, Vernetzung und KI-gestützte Betriebsprozesse kombiniert. Komplexe Hybrid- und Multi-Cloud-Umgebungen werden so sicher, effizient und transparent betrieben.