KI-GESTÜTZTEN EMAIL-BEDROHUNGEN *IMMER EINEN SCHRITT VORAUS*

> **Bedrohungen zu stoppen, bevor sie User erreichen, ist entscheidend für Sicherheit und Produktivität.**

Stefan Bast, IT Security Officer, Marquardt

MARQUARDT

ÜBERBLICK

Marquardt, ein globaler Hersteller von mechatronischen Systemen, stand vor der Herausforderung, die steigende Zahl an Phishing- und Spam-Mails zu bewältigen und gleichzeitig den Aufwand für das IT-Team zu reduzieren. Mit Advanced Email Security von Open Systems setzte das Unternehmen auf eine zentral gemanagte Lösung, die sich nahtlos in die bestehende Infrastruktur integriert. Ergebnis: Rund 25 % mehr verdächtige Emails blockiert, weniger False Positives und spürbar entlastete Security-Teams.

KUNDENDETAILS

- Produktionsgewerbe
- Rietheim-Weilheim, Deutschland
- 4 Kontinente
- 9,700
- marquardt.com

EINGESETZTE PRODUKTE

- Advanced Email Security
- Standard Email Security
- SD-WAN

ERGEBNISSE

810.000 €
SCHÄDEN
zusätzlich verhindert (pro Jahr)

<0.1%
FALSE POSITIVES

~6 Mio.
EMAILS FERNGEHALTEN
aus Mailboxen (pro Jahr)

+25%
GEBLOCKTE
verdächtige Emails

5.823
MAILBOXEN
geschützt (Nutzer)

Ca. 16 Mio.
EMAILS
gefiltert (pro Jahr)

Wir sprachen mit **Stefan Bast, IT Security Officer, und Philipp Schuster, IT Infrastructure Security bei Marquardt** über IT-Herausforderungen und -Zielsetzungen des Unternehmens – und darüber, wie Open Systems eine ganzheitliche Lösung ermöglicht hat.

WELCHE AUSWIRKUNGEN HABEN EMAIL-BEDROHUNGEN AUF IHRE SICHERHEITSSTRATEGIE?

Email-Bedrohungen spielen eine zentrale Rolle in unserer Sicherheitsstrategie, da sie nach wie vor das größte Einfallstor für Cyberangriffe darstellen. Sobald eine schadhafte Nachricht die technischen Schutzmaßnahmen passiert, hängt die Sicherheit am „schwächsten Glied" – dem Nutzer. Aus Unwissenheit, Stress oder Unachtsamkeit kann dieser auf manipulierte Links oder infizierte Anhänge klicken und so ungewollt eine Attacke auslösen. Deshalb betrachten wir Email-Security als einen der wichtigsten Bausteine unserer Verteidigungsstrategie.

Auch zahlreiche Reports bestätigen: Phishing-Angriffe werden zunehmend raffinierter – nicht zuletzt durch den Einsatz künstlicher Intelligenz. Täuschend echt gestaltete Emails, gezielte Social-Engineering-Taktiken und die Umgehung klassischer Filtermechanismen stellen selbst etablierte Sicherheitssysteme vor neue Herausforderungen. Aus diesem Grund sind wir hier von Anfang an besonders restriktiv vorgegangen. Beispielsweise filtern wir konsequent Anhänge heraus – ein aufwändiger, aber wirksamer Ansatz, der uns in der Vergangenheit bereits mehrfach vor gravierenden Schäden bewahrt hat.

WELCHE BEDROHUNG, HERAUSFORDERUNG ODER ZIELE HABEN SIE DAZU BEWEGT, EINE ERWEITERTE EMAIL-SICHERHEITSLÖSUNG WIE ADVANCED EMAIL SECURITY EINZUFÜHREN?

Wir haben uns entschieden, zusätzlich zum bereits leistungsstarken Standard Email Security Service von Open Systems sowie Microsoft 365 Defender auch Schutz vor besonders ausgeklügelten, gezielten und KI-gesteuerten Email-Bedrohungen aufzubauen, die etwa darauf abzielen, Anwender zur Preisgabe vertraulicher Informationen zu manipulieren. Die rein technische Authentifizierung, wie per SPF, DKIM oder DMARC reicht heute nicht mehr aus.

Deshalb haben wir mit Open Systems einen Proof of Concept durchgeführt, und die ersten Ergebnisse zeigten schnell, dass mit Advanced Email Security zusätzlich mindestens 15 % mehr gefährliche Emails herausgefiltert werden konnten.

> **Angreifer nutzen KI, um ihre Email-Attacken zu verbessern – deshalb brauchen wir KI-gestützten Schutz, der filtert, was Usern entgeht.**

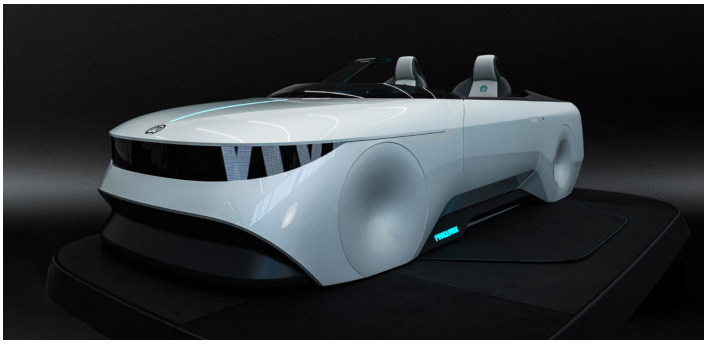
Philipp Schuster, IT Infrastructure Security

Die Bedrohungslage hat sich in den letzten Jahren deutlich verschärft. Angriffe sind raffinierter geworden, neue Methoden wie Phishing über QR-Codes stellen zusätzliche Risiken dar. Uns war daher klar: Wir müssen handeln. Am Ende ist es eine Frage des Risikomanagements.

Bei Marquardt ist Email-Security eines der Top 3 Risikothemen, mit finanziellen sowie Reputations-Risiken, und damit selbstverständlich auch auf Vorstandsebene eine Priorität.

WAS HAT SIE ÜBERZEUGT, SICH FÜR DIE ADVANCED EMAIL SECURITY SPEZIELL VON OPEN SYSTEMS ZU ENTSCHEIDEN?

Ausschlaggebend war für uns der globale Ansatz von Open Systems: Alle Services stammen aus einer Hand, laufen in einer gemeinsamen Infrastruktur und sind in einen Managed Service integriert. Der Service wird 24x7 abgedeckt und zusätzlich durch Customer Success Manager, die uns seit Jahren kennen, komplementiert. Hätten wir stattdessen eine zusätzliche single-point-solution, also eine externe Advanced Email Security Lösung eingesetzt, wäre das mit erheblichem Mehraufwand verbunden



gewesen – vom Einbinden in den bestehenden Email-Flow, die Infrastruktur bis zur Absicherung der Verfügbarkeit und der Reduzierung von Redundanzen. Für uns hätte das einen enormen betrieblichen Aufwand bedeutet. Bei Open Systems hingegen war es im Grunde nur das Aktivieren einer weiteren Lösung auf der Plattform.

Die Lösung integriert sich nahtlos in die bestehende Plattform. Über das Open Systems Portal – inklusive Incident-Tracking, Change Management und weiterer Funktionen – haben wir einen zentralen Anlaufpunkt, neben dem responsiven Operations Center "Mission Control". Für uns als Kunde ist das äußerst komfortabel: Wir benötigen nur einen einzigen Point of Contact und können dort alles abwickeln. Genau darin liegt für uns auch der Kern eines Managed Service – den eigenen Betriebsaufwand reduzieren und gleichzeitig das Know-how des Security-Providers optimal nutzen.

WIE HILFT DER MANAGED SERVICE VON OPENS SYSTEMS IHREM IT-TEAM?

Wir sind im Automobilgeschäft, einer Branche, die sich aktuell in einer wirtschaftlich angespannten Situation befindet. Entsprechend achten wir sehr genau auf Personalkosten – insbesondere in Hochlohnländern wie Deutschland.

Gerade deshalb ist ein Managed Service wie der von Open Systems für uns so wertvoll. Zum einen wäre es kaum möglich, kurzfristig die gleiche Qualität intern aufzubauen, wie sie ein spezialisierter Anbieter liefern kann. Zum anderen schätzen wir den durchgängigen 24x7-Vollservice, der konstant auf gleich hohem Niveau ist mit Level 3 Support. Das unterscheidet Open Systems deutlich von vielen Mitbewerbern, die außerhalb der regulären Arbeitszeiten lediglich eine Rufbereitschaft bieten.

> **Advanced Email Security ist ein hervorragendes Beispiel, wie Open Systems permanent das eigene Service Portfolio weiterentwickelt und neue Technologien und Lösungen integriert, und damit den Value-Add für die Kunden erhöht.**

Guido Wettemann, Director Global Operations IT-Systems

WIE VERLIEF DIE IMPLEMENTIERUNG VON ADVANCED EMAIL SECURITY UND WIE GUT HAT SICH DIE LÖSUNG IN IHRE BESTEHENDEN KOMMUNIKATIONS- UND SICHERHEITSPROZESSE INTEGRIERT?

Die Implementierung verlief dank des Learning Mode sehr reibungslos. In dieser Phase arbeitet das System für 1-2 Monate quasi im „Beobachtungsmodus": verdächtige Emails werden erkannt und markiert, aber noch nicht blockiert. So konnten wir genau nachvollziehen, welche Nachrichten herausgefiltert worden wären – ohne dass der Email-Verkehr tatsächlich beeinflusst wurde. Dadurch ließ sich die Lösung problemlos in Betrieb nehmen, ohne dass fälschlicherweise legitime Nachrichten blockiert wurden.

Im Anschluss haben wir in einem gemeinsamen Workshop konkrete Beispiele ausgewertet. Dabei zeigte sich, dass Advanced Email Security weitere verdächtige Nachrichten identifiziert hätte, die mit den bisherigen Mechanismen noch durchgegangen sind. Das war für uns ein klarer Beleg für die zusätzliche Schutzwirkung. False Positives waren äußerst selten – wir haben bislang unter 0.1% entdeckt. Inzwischen hat die Engine aber auch diese gelernt zu bewerten, sodass die manuelle Whitelist-Eintragung künftig entfallen kann. Dies entlastet unsere Service-Center und erhöht die Zufriedenheit der restlichen Mitarbeitenden, die sonst auf ihre Emails warten bzw. diese anfragen.

Die Endanwender haben die Umstellung selbst nicht bemerkt. Erst wenn eine Email fehlte, etwa im Fall eines False Positives, wurden sie aktiv. Unser Service Desk wurde entsprechend geschult, um in solchen Fällen zu prüfen, ob eine Nachricht fälschlicherweise abgefangen wurde, und den Vorgang bei Bedarf zu eskalieren.

WELCHE KONKRETEN VERBESSERUNGEN HABEN SIE SEIT DER EINFÜHRUNG FESTGESTELLT?

Seit der Einführung von Advanced Email Security werden rund 25 % mehr Emails zuverlässig abgefangen. Besonders auffällig ist, dass viele Massenmails und Phishing-Versuche, die früher noch durchgekommen sind, nun effektiv blockiert werden. Früher mussten wir bzw. unser CISO regelmäßig Rundmails versenden, um die Empfänger darauf hinzuweisen, gefährliche Nachrichten sofort zu löschen – heute kommt das deutlich seltener vor.

Insgesamt hat Advanced Email Security unsere Abwehr deutlich verbessert und verhindert, dass gefährliche Emails die Endanwender erreichen.

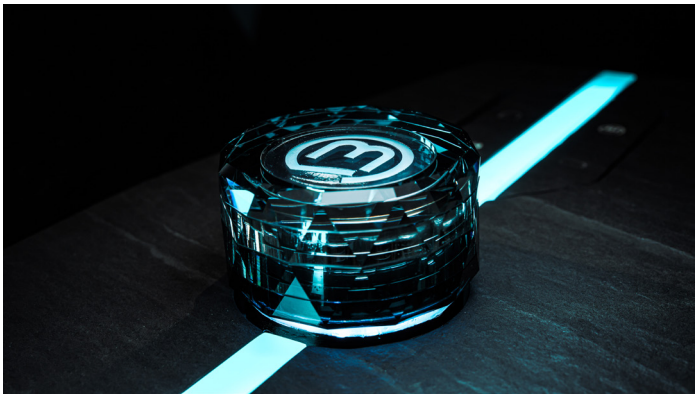
WIE HAT SICH IHRE EMAIL-SICHERHEITSLAGE VERÄNDERT, AUCH IN BEZUG AUF MITARBEITERSICHERHEIT UND AWARENESS?

Das ist schwer zu beurteilen, da der Endanwender von der Email-Sicherheit im Alltag kaum etwas mitbekommt – verdächtige Nachrichten werden kommentarlos herausgefiltert. Dadurch könnte das Gefahrenbewusstsein der Anwender nachlassen, weshalb unser CISO auch weiterhin regelmäßig alle Anwender schulen wird.

> **Email-Sicherheit ist der kritischste Angriffsvektor. Eine Investition in diesem Bereich ist eine der effektivsten Methoden, die Angriffsfläche zu reduzieren.**

Heiko Wirth, Chief Information Security Officer

Für uns als IT-Security-Team hingegen ist die Einführung von Advanced Email Security ein klarer Erfolg und es werden deutlich mehr Bedrohungen abgefangen. Neben besserer Erkennung hat auch das Ticketaufkommen spürbar abgenommen: Früher fragten Mitarbeitende regelmäßig nach, ob verdächtige Mails Spam seien – solche typischen Phishing-Mails erreichen sie



heute kaum noch. Das entlastet sowohl das Security-Team als auch die Anwender.

Derzeit haben wir zwar noch eine zusätzliche Sicherheitsstufe, da Nutzer Emails oft nur flüchtig lesen und Fälschungen übersehen. Deshalb können Spam-Mails derzeit nicht selbst freigeschaltet werden, sondern erfordern eine Freigabe durch den IT Service Desk.

Allerdings reduziert die Kombination der Schutzmechanismen das Risiko erheblich. Besonders überzeugt uns der KI-Einsatz, etwa bei der Analyse von Anhängen, Links oder QR-Codes, der Prüfung der Absender-Reputation sowie der Bewertung von Piktogrammen und Kommunikationsmustern. Advanced Email Security sammelt Hunderte von Signalen pro Email und gleicht sie mit dem Kontext des Unternehmens ab. Die Engine betrachtet den Kontext und lernt kontinuierlich dazu.

WELCHEN RAT WÜRDEN SIE ANDEREN UNTERNEHMEN GEBEN, DIE IHRE EMAIL-SICHERHEIT AUF EIN HÖHERES NIVEAU BRINGEN WOLLEN?

Unbedingt Advanced Email Security in Erwägung ziehen – und vor allem einen Proof of Concept durchführen. Nur so erhält man belastbare Fakten. Mit Bauchgefühl oder Angstargumenten überzeugt man keine Geschäftsführung. Vor dem Management zählen konkrete Zahlen.

Wichtig ist, die Tragweite klarzumachen: Eine erfolgreiche Attacke kann existenzbedrohend sein. In unserem Fall führten die Ergebnisse aus dem Proof of Concept, die klare Priorisierung durch unseren CISO und das Risikobewusstsein des gesamten Boards zur Freigabe – trotz angespannter wirtschaftlicher Lage.

Da man im Security-Umfeld nicht ständig neue Budgets fordern kann, müssen Prioritäten gesetzt werden. Email-Security ist für uns ein Top-Thema: Sie ist der wichtigste Angriffsvektor und für alle Mitarbeiter nachvollziehbar, da jeder beruflich wie privat mit Emails arbeitet.

MÖCHTEN SIE SONST NOCH ETWAS ÜBER IHRE ERFAHRUNG MIT EMAIL SECURITY ODER DIE ZUSAMMENARBEIT MIT OPEN SYSTEMS TEILEN?

Ein entscheidender Erfolgsfaktor von Open Systems ist für uns der All-Inclusive Service, der konstant auf hohem Niveau arbeitet sowie das breite Lösungsangebot auf einer Plattform. Zusätzlich ist es sehr wertvoll, dass wir jederzeit Zugriff auf ein Team von dedizierten Technical Account Managern haben. Diese Unterstützung im Hintergrund ist für uns äußerst wichtig und trägt erheblich zur Effizienz und Sicherheit unserer Email-Kommunikation bei.

Wir sind global aufgestellt und hatten vor Jahren noch an jedem Standort eine eigene Lösung im Einsatz. Zwar hatten wir klare Regeln definiert, wie der Email-Verkehr gehandhabt werden sollte, doch in der Praxis entwickelte sich das sehr uneinheitlich – Standards wurden nicht konsequent umgesetzt und Prozesse liefen auseinander.

Mit der zentralen Lösung von Open Systems haben wir jetzt eine einheitliche Plattform und profitieren zusätzlich vom 24x7-Support. Das bedeutet für uns: Wir werden nicht mehr nachts aus dem Schlaf geklingelt, sondern die einzelnen Standorte können sich direkt an Open Systems wenden, Vorfälle prüfen lassen oder zusätzliche Informationen einholen, wenn Unsicherheit besteht.

Zur Zusammenfassung ↓

Stefan Bast
IT Security Officer
Marquardt

Philipp Schuster
IT Infrastructure Security
Marquardt

AUF EINEN **BLICK**

DIE HERAUSFORDERUNG

Phishing-Angriffe werden immer raffinierter – nicht zuletzt durch AI, u.a. durch täuschend echt gestaltete Emails, gezieltes Social-Engineering und die Umgehung klassischer Filter. Marquardt stellte sich daher die Aufgabe, die wachsende Flut an Phishing- und Spam-Emails abzuwehren – trotz vorhandenem Schutz wie Secure Email Gateway (SEG) und Microsoft 365 Defender. Gleichzeitig sollte der operative Aufwand reduziert werden.

DIE LÖSUNG

Mit Advanced Email Security von Open Systems entschied sich Marquardt für eine zentrale, gemanagte Lösung, die sich nahtlos in die bestehende Infrastruktur integrieren ließ. Durch 24x7-Support, eine konsolidierte Plattform und intelligente Schutz-Engines wurde die Sicherheit entscheidend erhöht.

DIE ERGEBNISSE

Heute werden rund 25 % mehr potenziell schadhafte Emails zuverlässig blockiert, während False Positives auf <0.1% gesunken sind. Das Ticketaufkommen sank spürbar, Marquardt ist zusätzlich vor Phishingattacken geschützt und so stärker vor Reputations- sowie finanziellen Schäden. Dazu werden das IT Security-Team und die IT Service Center spürbar entlastet.

Über Marquardt
Die familiengeführte Marquardt-Gruppe mit Sitz in Rietheim-Weilheim, Deutschland, entwickelt und produziert seit 1925 mechatronische Schalter- und Bedienlösungen – u. a. für die Automobilindustrie, Haushaltsgeräte und Elektrowerkzeuge. Mit etwa 10.000 Mitarbeitenden an rund 21 Standorten weltweit erzielte die Gruppe 2024 einen Umsatz von etwa 1,4 Mrd. €

Open Systems bietet Managed SASE-Lösungen, die Netzwerk- und Sicherheitsfunktionen in einer cloudbasierten Plattform vereinen und hybride IT-Umgebungen sicher vernetzen – für mehr Effizienz, Sicherheit und maximale Skalierbarkeit.

Weitere Informationen unter **open-systems.com** |