DATENBLATT

FireEye Email Security Cloud Edition

Cloudgestützte Plattform zur Identifizierung, Analyse und Abwehr E-Mail-basierter Angriffe

HIGHLIGHTS

- Schützt ein- und ausgehende E-Mails
- Konsolidiert alle E-Mail-Sicherheitsmaßnahmen in einer Lösung
- Unterstützt YARA-Regeln für effizientere Bedrohungserkennung
- Leitet automatische Maßnahmen in Office 365 ein und entfernt E-Mails aus dem Posteingang eines Benutzers, wenn diese nach der Zustellung als schädlich erkannt werden.
- Unterstützt Verbindungen zu allen E-Mail-Anbietern
- Nutzt detaillierte Kenntnisse über Angreifer und deren Taktiken aus Incident-Response-Einsätzen und Beobachtungen von FireEye
- Erfüllt FedRAMP-Sicherheitsanforderungen

„E-Mails sind ein wesentlicher Teil jeder Zusammenarbeitsumgebung. FireEye Email Security ermöglicht uns, mit einer einzigen Lösung das Angriffsrisiko dieses für Hacker attraktiven Kanals zu minimieren.“

Nils Göldner
Managing Partner und Cloud Advisor
Blackboat GmbH

Überblick

Der größte Teil des eingehenden Datenverkehrs erreicht Unternehmen per E-Mail. Das macht E-Mail-Systeme verwundbar und damit ein beliebtes Einfallstor für Hacker. Unternehmen müssen nicht nur eine steigende Anzahl E-Mail-basierter Malware- und Spam-Angriffe, sondern auch immer mehr komplexe Bedrohungen abwehren, bei denen E-Mails missbraucht werden. Bei Letzteren enthalten die E-Mails zumeist Links zu Websites zum Stehlen von Anmeldedaten, betrügerische Überweisungsaufforderungen oder schädliche Anhänge. E-Mails sind auch deshalb der bevorzugte Angriffsvektor vieler Cyberkrimineller, weil sie ganz gezielt an bestimmte Personen oder Zielgruppen geschickt und genau auf diese zugeschnitten werden können.

Mit FireEye Email Security können Unternehmen all ihre E-Mail-Sicherheitsmaßnahmen in einer Lösung konsolidieren, um das Risiko kostspieliger Sicherheitsverletzungen zu minimieren und gleichzeitig die Kosten zu senken und die Mitarbeiterproduktivität zu steigern. FireEye Email Security ist eine funktionsreiche cloudbasierte Lösung, die sich unter anderem durch die zuverlässige Erkennung und Isolierung von Angriffen auszeichnet, die auf schädlichen URLs oder Anhängen oder auf der Vortäuschung falscher Absender basieren. Die Lösung blockiert diese Angriffe umgehend, noch bevor sie in die Infrastruktur des anvisierten Unternehmens gelangen. Mit der automatischen Löschfunktion für Office 365 können E-Mails, die nach der Zustellung als schädlich erkannt werden, aus dem Posteingang eines Benutzers entfernt werden. Darüber hinaus durchsucht FireEye Email Security ausgehende E-Mails nach Anzeichen für komplexe Bedrohungen, Spam und Viren.

Unsere skalierbare Big-Data-Plattform setzt von Plug-ins erfasste Daten und Kontextinformationen aus diversen Quellen zueinander in Beziehung, um in E-Mails enthaltene schädliche URLs zu identifizieren. Zudem prüft sie den Namen und die E-Mail-Adresse des Absenders auf Echtheit und den Inhalt der E-Mail auf gängige, zum Imitieren legitimer Absender genutzte Methoden, um CEO-Fraud und andere nicht auf Malware basierende Angriffe abzuwehren. Mithilfe der signaturunabhängigen MVX-Engine (Multi-Vector Virtual Execution™) gleicht sie E-Mail-Anhänge und URLs mit einer umfassenden Kreuzmatrix der Betriebssysteme, Anwendungen und Browser ab. Dadurch fallen bei der Bedrohungserkennung nur wenige nicht relevante Informationen an und es treten kaum Fehlalarme auf.

FireEye verfügt über detaillierte Bedrohungsdaten zu Hackern, die aus den von unseren Experten durchgeführten Bedrohungsuntersuchungen und aus Millionen von Sensoren stammen. Email Security nutzt diese Indizien und Kontextdaten zu Angriffen und Hackern, um Prioritäten für Warnmeldungen festzulegen und Bedrohungen in Echtzeit zu blockieren.

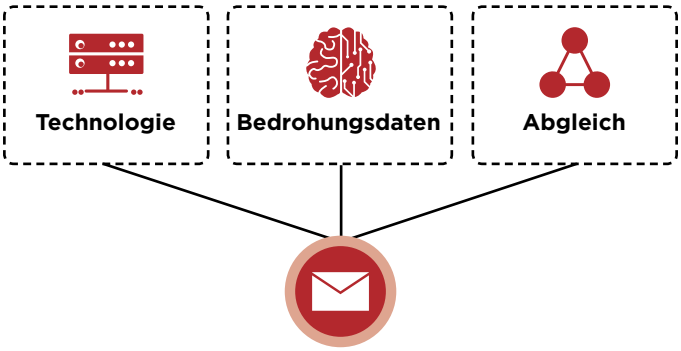

Abbildung 1: ein sicheres E-Mail-Gateway

Darüber hinaus kann Email Security in FireEye Network Security integriert werden, um einen umfassenderen Überblick zu bieten und Sicherheitsmaßnahmen in Echtzeit gegen kombinierte Angriffe mit mehreren Vektoren zu koordinieren.

Schutz vor E-Mail-basierten Bedrohungen

Cyberkriminelle recherchieren ihre Opfer mithilfe der unzähligen persönlichen Daten, die online frei verfügbar sind, bevor sie sich ihr Vertrauen mit Methoden des Social Engineering erschleichen. So können sie praktisch jeden dazu bringen, einen Link anzuklicken oder einen Anhang zu öffnen.

Typische Beispiele sind Spear-Phishing-Angriffe, E-Mails mit gefälschten Absendern und diverse Methoden zum Diebstahl von Anmeldedaten. Im Gegensatz zu den meisten herkömmlichen E-Mail-Sicherheitslösungen erkennt und blockiert FireEye Email Security diese Taktiken in Echtzeit. E-Mails werden analysiert und blockiert (in Quarantäne gesetzt), wenn neue oder komplexe Bedrohungen in Dateianhängen verschiedenster Art gefunden werden, unter anderem in:

- EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 sowie ZIP-, RAR- und TNEF-Archiven
- passwortgeschützten und verschlüsselten Anhängen
- in E-Mails eingebetteten URLs, PDFs und Microsoft-Office-Dokumenten
- URLs für Anmeldedaten-Phishing und Typosquatting
- unbekannten Sicherheitslücken in Betriebssystemen, Browsern und Anwendungen
- schädlichem Code in Spear-Phishing-E-Mails

Ransomware-Angriffe beginnen zwar mit einer E-Mail, aber vor der Verschlüsselung muss die Ransomware eine Verbindung zu einem Command-and-Control-Server herstellen. Email Security erkennt und stoppt diese schwer aufspürbaren, mehrstufigen Malware-Kampagnen.

Überlegene Bedrohungserkennung

Email Security hilft Unternehmen dabei, im normalen Internet-Datenverkehr versteckte, komplexe, gezielte und auf die Umgehung von Sicherheitsmaßnahmen ausgelegte Angriffe zu erkennen und zu blockieren und damit das Risiko kostspieliger Sicherheitsverletzungen zu senken. Angriffe werden unmittelbar nach der Aufdeckung gestoppt und analysiert. Dabei wird ein digitaler Fingerabdruck erstellt, um denselben Angriff in Zukunft schneller zu erkennen.

Kernkomponenten von Email Security sind die leistungsstarken URL-Sicherheitsfunktionen von Advanced URL Defense und die MVX-Engine. Beide nutzen brandaktuelle maschinelle Lernverfahren und Analysefunktionen, um Angriffsmethoden zu erkennen, die herkömmliche, auf Signaturen oder Richtlinien basierende Sicherheitsmaßnahmen umgehen.

Integraler Bestandteil der Sicherheitsfunktionen von Advanced URL Defense ist PhishVision, ein Algorithmus zur Klassifizierung von Bilddateien. Dieser erfasst und speichert Screenshots der Anmeldeseiten und anderer Webseiten legitimer, aber häufig angegriffener Marken und vergleicht sie mithilfe von Deep-Learning-Verfahren mit den in E-Mails enthaltenen URLs. Ergänzend zu PhishVision wird das Plug-in Kraken eingesetzt, das Domains und Seiteninhalte analysiert, um Phishing-Angriffe zu erkennen und die maschinellen Lernverfahren zu verbessern. Ein weiteres innovatives Tool zur Erkennung schädlicher URLs ist Skyfeed, ein speziell für diesen Zweck erstelltes, vollständig automatisiertes System, das Informationen über Malware erfasst und speichert. Skyfeed sammelt unter anderem Konten in sozialen Netzwerken, Blogs, Foren und Bedrohungsdaten-Feeds, um die fehlerhafte Klassifizierung schädlicher Inhalte zu vermeiden. Mit diesem mehrgleisigen Ansatz schützt Advanced URL Defense Unternehmen zuverlässig vor Spear-Phishing-Angriffen und dem Diebstahl von Anmeldedaten.

Angreifer verwenden gern harmlos wirkende E-Mails, die im Posteingang des Benutzers landen und sich erst nach der erfolgreichen Zustellung als schädlich herausstellen. Email Security Cloud Edition untersucht E-Mails auch noch zu diesem Zeitpunkt und löst bei Bedarf eine Warnmeldung aus. Über die API für Office 365 kann eine Richtlinie erstellt werden, damit E-Mails mit nachträglich aktiviertem Schadcode automatisch aus dem Posteingang entfernt werden.

Die MVX-Engine identifiziert Zero-Day-Exploits, Multi-Flow-Angriffe und andere gut getarnte Angriffe mithilfe dynamischer, signaturunabhängiger Analysen in sicheren, virtuellen Umgebungen. Sie ermöglicht die Identifizierung bisher vollkommen unbekannter Exploits und Malware, sodass Angriffe bereits in den ersten Phasen des Angriffszyklus gestoppt werden können.

Besserer Schutz vor Spam und Viren

FireEye Email Security Cloud Edition kann mit Anti-Spam- und Antivirensoftware (AVAS) ausgestattet werden, um gängige Angriffe und E-Mails mit gefälschtem Absender mithilfe eines konventionellen Signaturabgleichs zu erkennen.

CEO-Fraud und andere Angriffe mit gefälschten Identitäten (die mitunter auch als Business E-Mail Compromise oder kurz BEC bezeichnet werden) fügen Unternehmen weiterhin erheblichen finanziellen Schaden zu. Das liegt zum Teil daran, dass diese Angriffe nicht auf Malware, sondern auf Social-Engineering-Methoden basieren. Die E-Mails enthalten deshalb keine schädlichen Anhänge oder Links, an denen sie erkannt werden könnten. Deshalb hat FireEye innovative Algorithmen, Systeme und Tools für die Erkennung und Abwehr von Angriffen entwickelt, die auf der Nutzung gefälschter Identitäten beruhen.

So ist beispielsweise Vorsicht geboten, wenn die Domain des Absenders noch sehr neu ist. Zu Beginn einer BEC-Kampagne richten die Angreifer eine Domain ein, die so ähnlich aussieht wie die der Person oder des Unternehmens, als die/das sie sich ausgeben wollen. Meist beginnen sie wenige Stunden später damit, E-Mails von dieser Domain aus zu verschicken.

Email Security nutzt die von FireEye entwickelten Tools Newly Existing Domains (NED) und Newly Observed Domains (NOD), um das Alter und den Reifegrad der Absenderdomain zu ermitteln. E-Mails von neuen Domains werden als verdächtig eingestuft und gründlich nach weiteren Hinweisen auf einen Angriff untersucht, darunter Typosquatting und Absenderanzeige- oder Benutzernamen-Spoofing.

Doch nicht alle Angreifer machen sich die Mühe, eine Domain zu kaufen und zu registrieren. Viele ändern einfach nur den angezeigten Absender oder den Nutzernamen, damit es so aussieht, als ob die E-Mail von einem vertrauenswürdigen Absender stammt. Daher prüft FireEye Email Security die Echtheit der angezeigten Absender- und Benutzernamen mithilfe eines Verzeichnisses für Anzeigenamen.

Prüfung ausgehender E-Mails

Ein Beispiel für die raffinierten Bedrohungen, die Email Security erkennt und abwehrt, sind schädliche Anhänge und Phishing-URLs, die durch ausgehende E-Mails verbreitet werden. Ausgehende E-Mails werden zudem auch nach Malware und Spam durchsucht, um zu verhindern, dass die Absender-Domains auf Blacklists gesetzt werden.

Aussagekräftige Warnmeldungen für eine wirksamere Bedrohungsabwehr

FireEye Email Security analysiert alle E-Mail-Anhänge und URLs, um moderne, komplexe Angriffe zu identifizieren. Das Gateway wird in Echtzeit mit Daten aus der gesamten FireEye-Installationsbasis aktualisiert, damit Warnmeldungen mit Kontextinformationen angereichert werden und bei Bedrohungen den mutmaßlichen Urheber identifizieren können. So können Sie die wichtigsten Warnmeldungen identifizieren, rechtzeitig auf sie reagieren und komplexe E-Mail-basierte Angriffe abwehren. Email Security deckt bekannte und unbekannte Bedrohungen sowie Angriffe auf, bei denen keine Malware verwendet wird. Dabei generiert es nur wenige nicht relevante Informationen und Fehlalarme, sodass Sie Ihre Ressourcen gezielt für die Abwehr tatsächlicher Angriffe einsetzen und so Betriebskosten sparen können.

Schnelle Anpassung an die sich ständig ändernde Bedrohungslage

Mit Email Security kann Ihr Unternehmen seine Abwehrmaßnahmen gegen E-Mail-basierte Bedrohungen kontinuierlich und proaktiv stärken. Email Security erstellt eigene Bedrohungsdaten, statt sich auf die oft zu spät eintreffenden Bedrohungsdaten-Feeds anderer Anbieter zu verlassen. Unseren Experten für E-Mail-Sicherheit und Bedrohungsanalysen stehen hauseigene, E-Mail-spezifische Bedrohungsdaten (Smart DNS) und Funktionen zur Datenerfassung zur Verfügung, sodass sie die Tools zur Erkennung von Spam, Angriffen mit gefälschten Identitäten usw. ständig weiterentwickeln können. Email Security setzt alle uns vorliegenden Daten zu Angreifern, Geräten und Opfern zueinander in Beziehung zur:

- Bereitstellung eines zeitnahen und umfassenden Überblicks über die Bedrohungen
- Identifizierung spezifischer Funktionen und Merkmale erkannter Malware und schädlicher Anhänge
- Bereitstellung von Kontextdaten, um Abwehrmaßnahmen zu priorisieren und zu beschleunigen
- Ermittlung möglicher Identitäten und Motive der Hacker und Nachverfolgung ihrer Aktivitäten in Ihrem Unternehmen
- Rückwirkenden Identifizierung von Spear-Phishing-Angriffen und Blockierung des Zugriffs auf Phishing-Websites durch das Überschreiben schädlicher URLs

Sicherheitsverantwortliche in Unternehmen können im Email-Security-Portal in Echtzeit eine Übersicht über Warnmeldungen erhalten sowie eigene Regeln und Berichte erstellen. Mithilfe dieser von Ihnen erstellten Regeln können Sie detaillierte, genau auf Ihre Situation abgestimmte Sicherheitsrichtlinien und -regeln definieren und durchsetzen.

Integration in die Prozesse zur Bedrohungsabwehr

Email Security arbeitet mit verschiedenen anderen FireEye-Lösungen zusammen, um die Prozesse zur Bearbeitung von Warnmeldungen zu automatisieren.

FireEye Central Management gleicht die Warnmeldungen von Email Security und Network Security ab, um einen umfassenderen Kontext des Angriffs zu gewinnen und Abwehrregeln zu definieren, die eine Ausbreitung verhindern.

FireEye Helix arbeitet reibungslos mit Email Security zusammen und vereinfacht, integriert und automatisiert die Sicherheitsmaßnahmen.

Einfache Installation und unternehmensweiter Schutz

FireEye Email Security Cloud Edition wird in der Cloud bereitgestellt, sodass keine zusätzliche Hardware oder Software installiert werden muss. Es ist perfekt für Unternehmen geeignet, die ihre E-Mail-Infrastruktur in die Cloud verlagern. Somit entfällt der Aufwand, der mit der Anschaffung, Installation und Verwaltung einer physischen Infrastruktur verbunden wäre.

FireEye Email Security Cloud Edition kann nahtlos in cloudbasierte E-Mail-Systeme wie Microsoft Office 365 mit Exchange Online Protection oder G Suite integriert werden.

Zum Schutz vor schädlichen E-Mails müssen Unternehmen nur die Nachrichten über Email Security leiten. Dort werden diese dann zuerst auf Spam und bekannte Malware untersucht. Anschließend kommen die URL-Sicherheitsfunktionen zum Einsatz. Sie prüfen alle Anhänge und URLs mithilfe der signaturunabhängigen MVX-Engine in einer sicheren Umgebung, um Bedrohungen zu erkennen und komplexe Angriffe in Echtzeit zu vereiteln.

Weitere Funktionen

Individuelle Anpassung mithilfe von YARA-Regeln

In Email Security können Analysten eigene YARA-Regeln definieren, um die Bedrohungserkennung zu verwalten und zu verbessern, neu erkannte Bedrohungen aufzudecken und ihr Unternehmen vor aktuell laufenden Angriffskampagnen zu schützen.

Aktiver Schutzmodus oder reine Überwachung

Email Security kann E-Mails analysieren und Bedrohungen isolieren. Dazu müssen Unternehmen lediglich ihre MX-Einträge so anpassen, dass Nachrichten an FireEye weitergeleitet werden. Im Überwachungsmodus muss nur eine transparente BCC-Regel eingerichtet werden, damit Kopien aller E-Mails zur MVX-Analyse an FireEye gesendet werden.

Autorisierungs- und Compliance-Zertifikate

ISO 27001

FireEye Email Security Cloud Edition erfüllt die Anforderungen der internationalen Norm ISO 27001 für das Informationssicherheitsmanagement in Rechenzentren.

FedRAMP

FireEye Email Security Cloud Edition mit AVAS-Schutz erfüllt die FedRAMP-Sicherheitsanforderungen für Cloud-Services in staatlichen und öffentlichen Bildungseinrichtungen.

SOC 2 Typ II

FireEye Email Security Cloud Edition ist mit der SOC 2 Typ II-Zertifizierung (Service Organization Controls) für Sicherheit und Vertraulichkeit des American Institute of Certified Public Accountants (AICPA) konform.

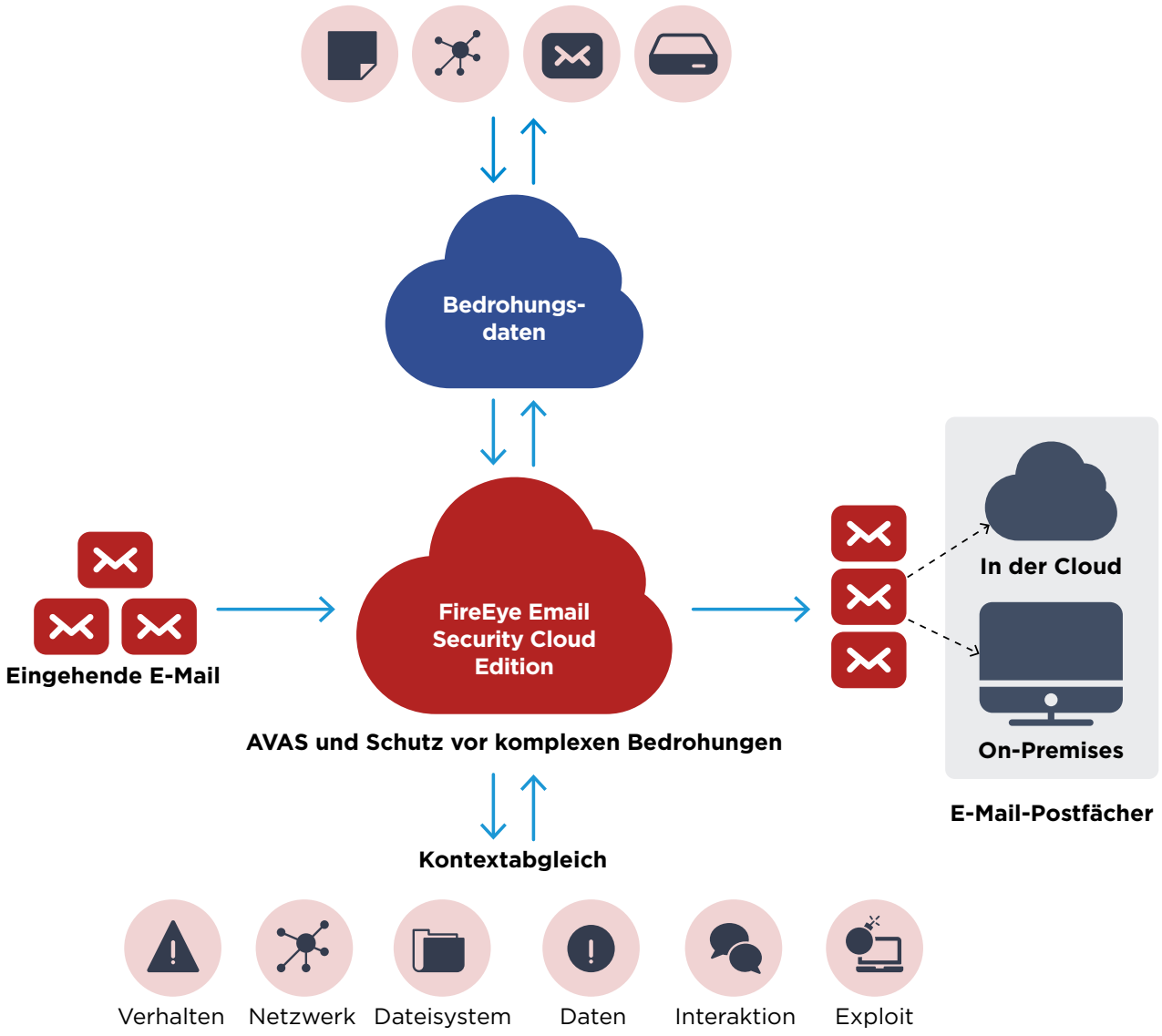

Abbildung 2: FireEye Email Security Cloud Edition

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de.**

Telecom Liechtenstein AG
Schaanerstrasse 1
9490 Vaduz / Liechtenstein
security@telecom.li
+423 237 90 90

Über FL1

Als erster konvergenter Full-Service-Provider Liechtensteins ergänzt FL1 damit sein Portfolio sowie sein strategisches Geschäftsfeld um Managed Security Services der nächsten Generation. Im Mittelpunkt steht die zeitnahe Erkennung von Risiken für die Sicherheit der IT von Unternehmen und Behörden als Solution oder als Managed Service. Basis dafür ist eine hochmoderne, eigenentwickelte Technologie-plattform mit welcher Kunden ihr Cyber Defence Centre (CDC) aufbauen können oder die in Kombination mit Security-Analyseexperten, bewährten Prozessen und Best Practices als CDC as a Service zur Verfügung steht.