IKARUS security software

IKARUS mail.security

Datenblatt

E-Mail-Sicherheit mit ATP-Option

Dank weltweit führender Security-Technologien erkennt IKARUS mail.security nicht nur Viren, Malware und schädliche Anhänge in E-Mails: Auch manipulierte URLs, Schadcode, Phishing- Versuche und Zero-Day-Attacken werden geblockt, bevor die Angriffe Ihr Netzwerk erreichen.

E-Mails stellen einen der häufigsten Angriffsvektoren für Cyber-Angriffe dar. IKARUS mail.security, die cloudbasierte Security-Lösung für E-Mail-Gateways, filtert und blockiert Spam, Malware und Phishing-Versuche in Echtzeit, noch bevor diese in Ihre Systeme eindringen und Schaden anrichten können. Das ATP-Add-On schützt mit Sandboxing-Technologien auch vor gezielten Angriffen.

Einfallstor Posteingang: immer mehr APT-Attacken

Ransomware-Attacken oder gezielte hochtechnisierte Angriffe (APT - Advanced Persistent Threats) sind häufig persönlich adressiert und flexibel an das Zielsystem angepasst. Manche nutzen plausible Attachments wie Rechnungen zu tatsächlich getätigten Einkäufen oder Bewerbungsschreiben auf aktuelle Stellenangebote, andere kommen ohne Malware und nur mit einer verlockenden URL, hinter der der tatsächliche Schadcode wartet.

Finden die Angreifer einen Weg ins System, verhalten sie sich unauffällig, um möglichst lange unentdeckt („persistent“) zu bleiben. Erst werden weitere Schwachstellen im System identifiziert, danach passende Schadensroutinen nachgeladen.

Verzögerungs- und Verschleierungstaktiken

Diese verzögerte Dynamik und das Ausnutzen von möglichst neuen, ungepatchten Schwachstellen erschweren die Erkennung dieser Angriffstaktik stark. Mit mehrstufigen dynamischen Analysen reduziert IKARUS mail.security das Risiko von Eindringlingen auf ein absolutes Minimum und verschafft Ihnen Klarheit darüber, ob Sie sich aktuell im Visier von Angreifern befinden.

Mit einer der weltweit besten Malware Scan Engines zur erweiterten Inhaltsanalyse, dem Advanced URL Defense-Feature zur Erkennung verzögerter Phishing-Angriffe sowie dem ergänzenden ATP-Add-on bietet IKARUS mail. security größtmögliche Sicherheit für Ihren SMTP-Traffic. Ein zentrales Dashboard bietet einen flexiblen Zugriff und schnellen Überblick über alle Security-Services, den Geräte- und Netzwerkstatus sowie Statistiken und Analysen.

Multi-Sandbox Ansatz

E-Mails, die nach wiederholten Analysen der IKARUS Malware Scan Engine weder als schädlich noch als harmlos eingestuft wurden, können zusätzlich mit dem signaturlosen Sandboxing-Ansatz von Trellix und anderen Marktführern überprüft werden. Für die Sandbox-Analysen durch ausgewählte Partner-Technologien werden nur jene Daten, bei denen die IKARUS Malware Scan Engine zu keinem endgültigen Ergebnis kommt, parallel erneut überprüft – diese liegen zumeist im Promillebereich des gesamten Datenvolumens. Der gezielte ergänzende Einsatz der Sandboxes ermöglicht auch kleinen und mittleren Unternehmen leistbaren Zugang zu dieser Technologie sowie ein höchstmögliches Schutzniveau. Die Sandboxes unserer Technologie-Partner sind im IKARUS Scan Center installiert: Alle Daten – gesendet werden DSGVO-konform nur Meta-Daten wie Anhänge oder Scripts – bleiben daher in Österreich. Die Sandboxes selbst empfangen zwar laufend Updates, können aber keine Daten versenden.

Post Incident Management und Advanced URL Defense

Sollte es einem Angreifer trotz mehrstufiger Abwehrbarrieren gelingen, seinen Code erfolgreich via E-Mail zu platzieren, läuft die Zeit gegen ihn: IKARUS mail.security überprüft mit jedem Update bis zu 14 Tage lang auch bereits zugestellte Anhänge auf Malware. Bei einem Sicherheitsvorfall – also einer zugestellten E-Mail, die zum Zeitpunkt des Empfangs noch nicht als bösartig identifiziert wurde – alarmiert das Post-Incident Management-System unverzüglich.

Mit Aktivierung des Features Advanced URL Defense scannt IKARUS mail.security Links nicht nur beim Empfang der E-Mail, sondern erneut bei jedem Anklicken der URL. So werden auch verzögerte Angriffe erkannt und abgewehrt. Damit bietet IKARUS den derzeit effizientesten Schutz vor Malware, Spam und gezielten Angriffen. EU-DSVGO-konform, kostengünstig und ohne zusätzlichen technischen Aufwand Ihrerseits.

Maximale Datensicherheit und Benutzerfreundlichkeit

Ihr zusätzliches Plus an Datensicherheit: Die Software-Entwicklung, Datenverarbeitung, Analyse und Support für IKARUS mail.security erfolgen in Österreich unter penibler Einhaltung der europäischen Datenschutzgrundverordnung. Es werden keine Daten an Dritte weitergegeben, alle Analysen – inklusive Sandbox-Analysen durch Partner-Unternehmen finden ausnahmslos im Rechenzentrum in Wien statt.

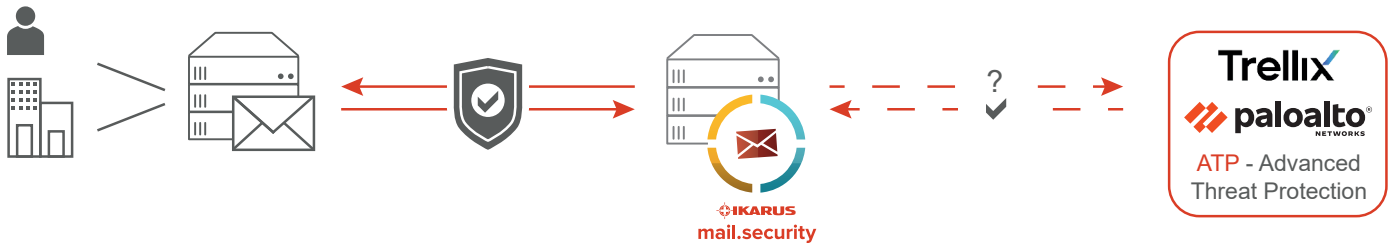

Abb. 1 - IKARUS mail.security scannt alle eingehenden E-Mails, bevor Sie an Ihr Netzwerk übergeben werden. Die Sandboxes von Trellix und PaloAlto zur Advanced Threat Protection können optional zugeschalten werden.

Vorteile

- Echtzeit-Schutz mit höchster Erkennungsleistung, optimiert auf schnellste Scan- und Reaktionszeiten
- Hocheffiziente globale Threat Intelligence dank internationaler Daten und Partnerschaften
- Mehrstufige verhaltensbasierende Analysen durch eigenen Simulator und Multi-Sandbox-Integration
- Automatisierte Reports & Statistiken zur Bedrohungslage sowie detailliertes Logging über alle Funktionen
- Hochprofessionelle skalierbare Lösung, multimandantenfähig und individuell adaptierbar
- Temporäre Archiv-Lösung für ein- und ausgehende E-Mails
- Multimandantenfähigkeit mit anpassbarem Admin- und User-Interface

Highlights

- Anti-Spam-Konzept mit Greylisting, bayesischer & lexikalischer Analyse, SPF u.a.
- Verhaltensbasierende Analysen von ausführbaren Dateien, Makros, Skripts, Archiven
- Erweiterte Link-Analyse sowohl bei E-Mail-Zustellung als auch erneut bei Klick auf den Link (Advanced URL Defense)
- Post Incident Management mit Alerting-Funktion
- Adaptives Spam-Bewertungssystem sowie kundenspezifische Filter und Aktionen
- Flexible Konfigurationsmöglichkeiten mit Black- und Whitelists und flexiblen Filteroptionen
- TLS-Verschlüsselung

»Die Software von IKARUS reagiert extrem schnell auf lokale Bedrohungen und hat uns dadurch bereits vor unzähligen Attacken bewahrt – sie ist ein fixer Bestandteil unseres Sicherheitskonzepts.«

Ing. Janusz Russocki - IT-Leiter der WITTMANN Gruppe

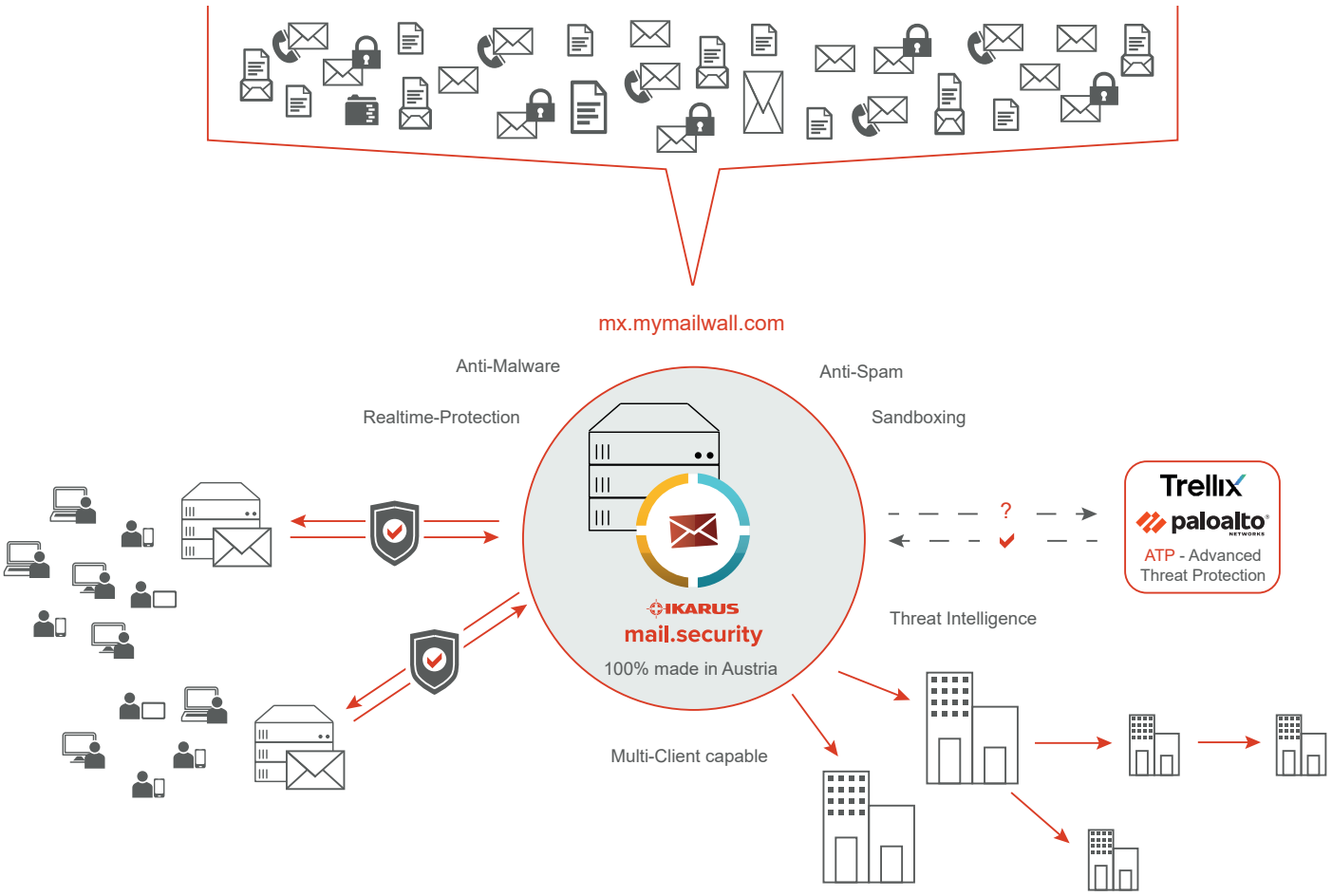

Abb. 2 - IKARUS mail.security mit ATP-Option: Anti-Malware, Anti-Spam, Attachment-Filter & Sandboxing

Systemanforderungen

- Internetverbindung
- Eigene E-Mail Domain

Über IKARUS Security Software

IKARUS Security Software kennt seit 1986 die Anforderungen von Admins, CIOs, Cert-Teams und ISPs an sichere IT- und OT-Systeme. Der österreichische Security-Spezialist entwickelt und betreibt zukunftsfähige Lösungen von der eigenen Scan Engine über Managed Security Services bis hin zu SOC/SiEM-Services in IT, IoT und OT (ICS) Umgebungen. Technologische Partnerschaften mit den Marktführern ihrer Bereiche verbinden globale Threat Intelligence mit den Vorteilen eines zentralen Ansprechpartners sowie lokaler Datenverarbeitung.