IKARUS security software

IKARUS mail.security

**Datenblatt**

# E-Mail-Sicherheit mit ATP-Option

Dank weltweit führender Security-Technologien erkennt I**KARUS 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.

Die cloud-basierte leistungsstarke Sicherheitslösung für E-Mail-Gateways sichert das Haupteinfallstor für Spam, Malware und Phishing-Versuche. Mit Echtzeit-Schutz, ATP-Add-on und unbegrenzten rekursiven Archiv-Scans blockiert IKARUS mail.security unbemerkt unerwünschte E-Mails, Schadcode und manipulierte Links, noch bevor diese in Ihre Systeme eindringen und Schaden anrichten können.

## Einfallstor Posteingang: immer mehr APT-Attacken

Ransomware-Attacken oder gezielte hochtechnisierte Angriffe (APT - Advanced Persistent Threats) sind häufig persönlich adressiert und flexibel an das ausgewählte Unternehmen 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 aktuellen, ungepatchten Schwachstellen erschweren die Erkennung eines erfolgreichen Angriffes stark. Mit gezielten mehrstufigen 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 Carrier-grade Scan Engines zur erweiterten Inhaltsanalyse, dem Advanced URL Defense-Feature zur Analyse manipulierter Links und Websites sowie dem ergänzenden ATP-Add-on bietet IKARUS mail.security größtmögliche Sicherheit für Ihren SMTP-Traffic. E-Mails, die nach hunderten Reputation- und Content-based Checks weder als schädlich noch als harmlos eingestuft wurden, können zusätzlich zu den dynamischen und heuristischen Analyseverfahren der IKARUS scan.engine mit dem signaturlosen Sandboxing-Ansatz von FireEye und anderen Marktführern überprüft werden. Der gezielte Einsatz dieser erweiterten Analysetechniken ermöglicht auch kleinen und mittleren Unternehmen leistbaren Zugang zu hochprofessionellen Sicherheitsvorkehrungen und ein höchstmögliches Schutzniveau.

## Maximale Datensicherheit und Benutzerfreundlichkeit

Zusätzliches Plus für Ihre Datensicherheit: Die Software-Entwicklung, Datenverarbeitung, Analyse und Support erfolgen in Österreich unter penibler Einhaltung der europäischen Datenschutzgrundverordnung. Es werden keine Daten an Dritte weitergegeben, alle Analysen finden ausnahmslos im Rechenzentrum in Wien statt. 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 und Post-Incident Management

Auch für die erweiterten ATP-Analysen durch Partner-Technologien werden nur jene Daten, bei denen die IKARUS scan.engine zu keinem verlässlichen Schluss kommt, parallel erneut überprüft – diese liegen zumeist im Promillebereich des gesamten Datenvolumens. 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 holen zwar laufend Updates vom Hersteller, sind aber abgeschottet, sodass sie nicht nach Hause telefonieren können.

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 E-Mails, Anhänge und URLs. Bei einem Sicherheitsvorfall – also einer zugestellten E-Mail, die zum Zeitpunkt der Zustellung noch nicht als bösartig identifiziert werden konnte – alarmiert das Post-Incident Management-System unverzüglich. Damit bietet IKARUS den derzeit effizientesten Schutz vor Malware, Spam und gezielten Angriffen. EU-DSVGO-konform, kostengünstig und ohne zusätzlichen technischen Aufwand Ihrerseits.

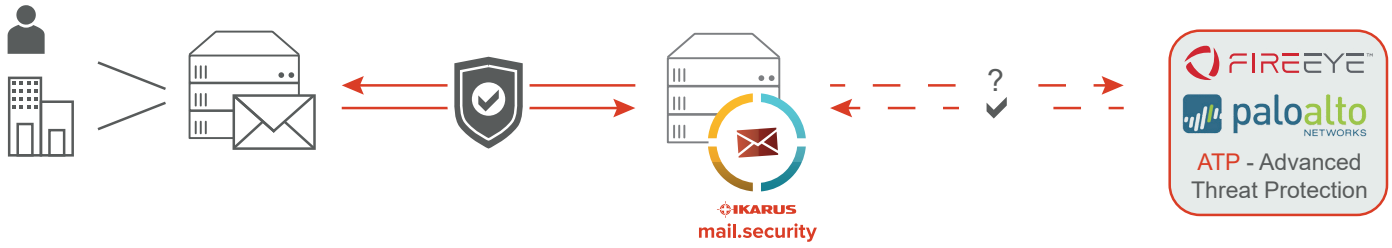


Abb. 1 - **IKARUS mail.security** scannt alle ein- und ausgehenden E-Mails, bevor Sie an Ihr Netzwerk übergeben werden. Die Sandboxes von FireEye und PaloAlto können optional zugeschalten werden.

## Vorteile

- Hochprofessionelle skalierbare Lösung, multimandantenfähig und individuell adaptierbar
- 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 integrierte Sandboxes
- Automatisierte Reports & Statistiken zur Bedrohungslage sowie detailliertes Logging über alle Funktionen
- Temporäre Archiv-Lösung für ein- und ausgehende E-Mails sowie Post Incident Alerts

## 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)
- Adaptives Spam-Bewertungssystem sowie kundenspezifische Filter und Aktionen
- Flexible Konfigurationsmöglichkeiten mit Black- und Whitelists und flexiblen Filteroptionen
- TLS-Verschlüsselung
- Multimandantenfähig mit anpassbarem Admin- und User-Interface

*»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

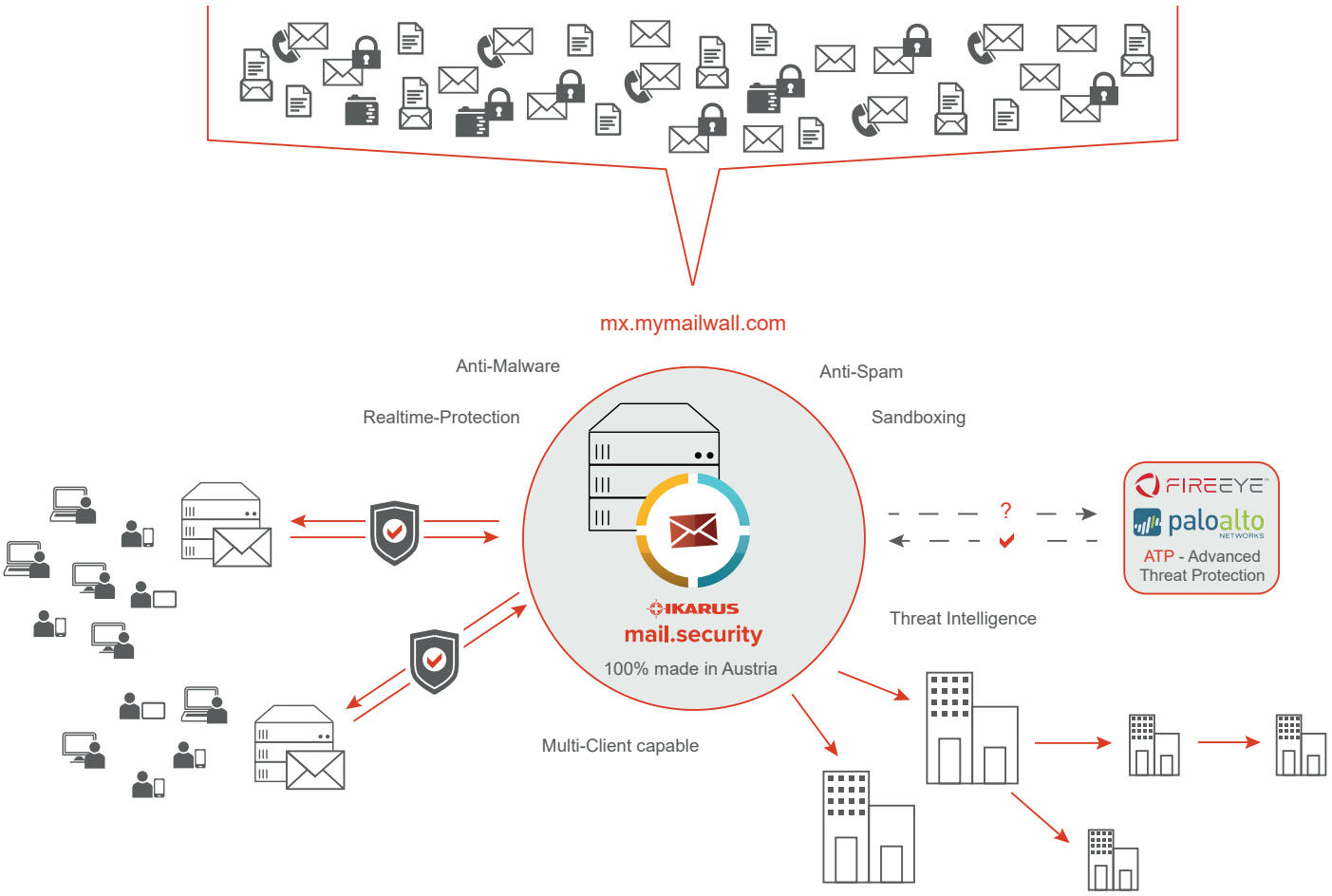


Abb. 2 - IKARUS mail.security mit ATP-Option: Anti-Malware, Anti-Spam, Attachment-Filter & Sandboxing

## Systemanforderungen

- Internetverbindung
- Eigene E-Mail Domain

PARTNER BUNDESBESCHAFFUNG BBG

## 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.