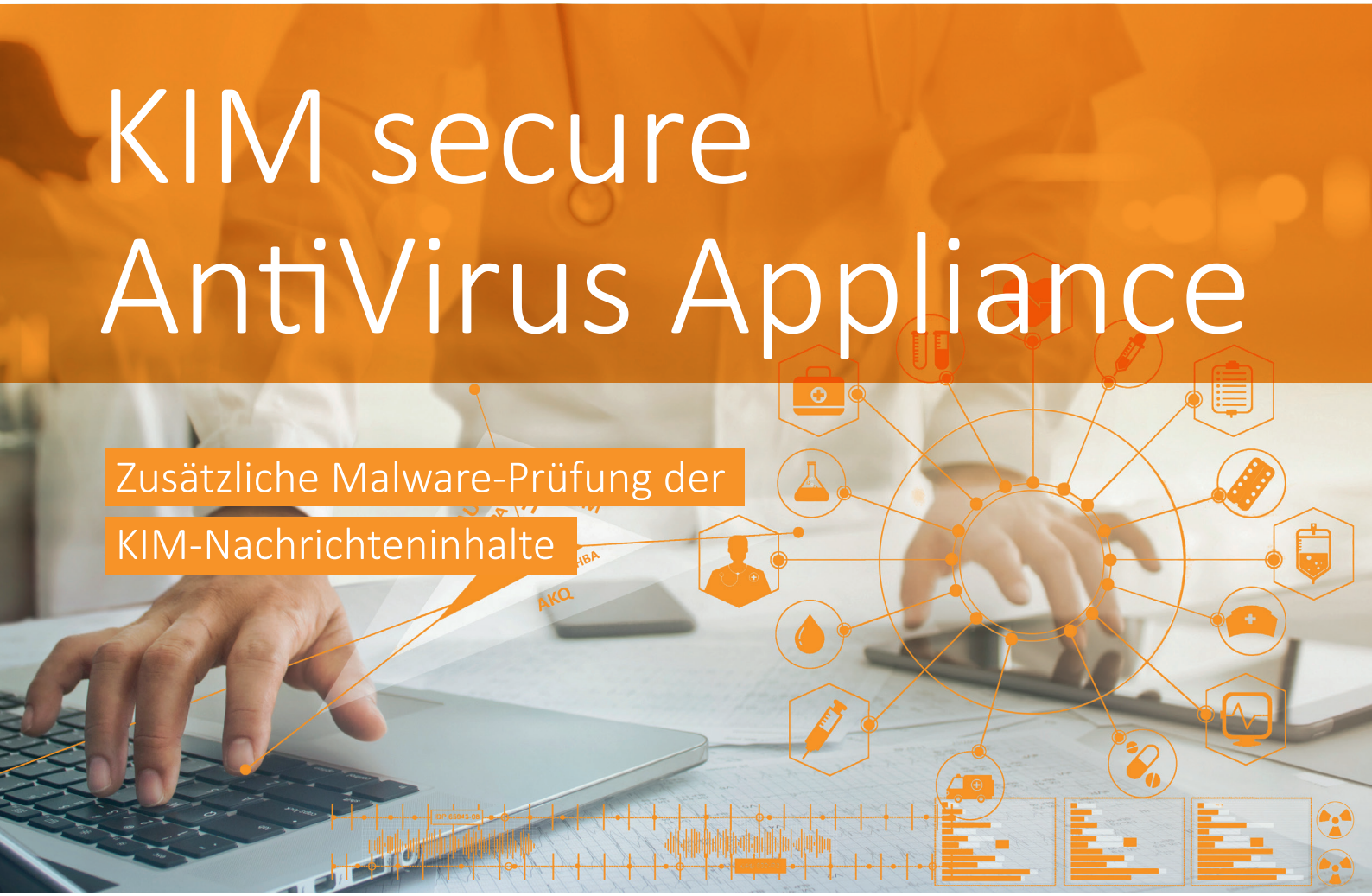
KIM secure AntiVirus Appliance

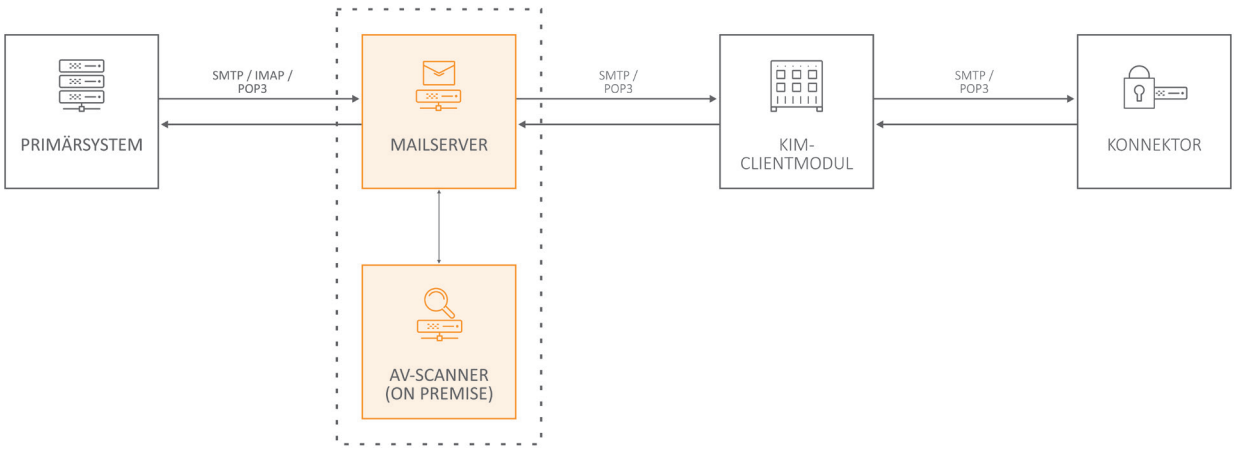


Zusätzliche Malware-Prüfung der KIM-Nachrichteninhalte

Die Anforderung

In der E-Mail-Kommunikation über KIM (Kommunikation im Medizinwesen) werden Daten aus Gründen der Sicherheit ausschließlich Ende-zu-Ende verschlüsselt übermittelt. Verschlüsselte Daten können in der Telematikinfrastruktur (TI) aber nicht auf Malware geprüft werden, weshalb grundsätzlich ein Restrisiko auf schadhaften Inhalt besteht. Eine Sicherheitscheck der Daten kann daher ausschließlich entweder nach der Entschlüsselung oder vor der Verschlüsselung erfolgen. Die Ver- und Entschlüsselung wird durch das KIM Clientmodul gesteuert.

Probleme können auch durch einen zusätzlichen MTA/Mail-Server als Proxy vor dem KIM Clientmodul entstehen, was weiteren Aufwand für Betrieb und Verwaltung bedeutet. Die spezifische Festlegung von KIM ermöglicht außerdem eine nur stark eingeschränkte Nutzung. Unter anderem ist die Angabe von KIM-Benutzernamen somit teilweise nicht möglich. Es erfolgt darüber hinaus ein zusätzliches, proprietäres Mapping von E-Mail-Konten zu KIM-Konten, Schadsoftware befindet sich ggf. bereits in der Systemumgebung des Empfängers. Teilweise übermitteln integrierte AntiVirus-Scanner auch Daten an Dritte.



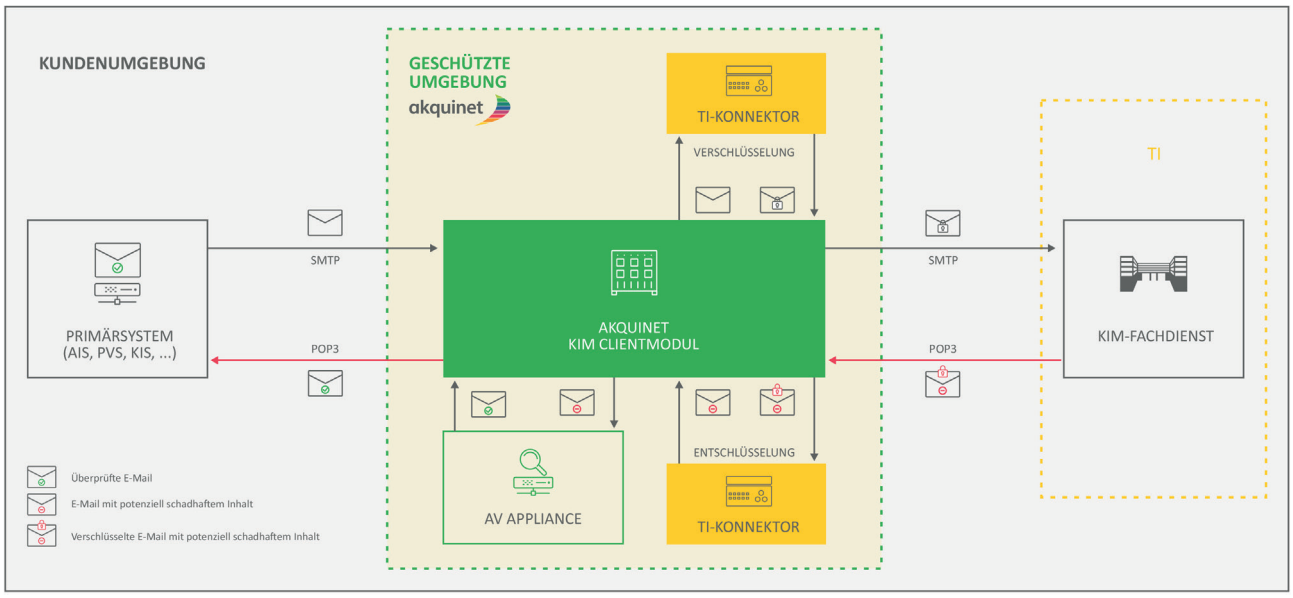
Die Lösung

Die Steuerung der Prüfung auf Schadsoftware erfolgt durch KIM Clientmodul. Es ist die erste Instanz, welche im Verlauf des Nachrichtenabrufs über die unverschlüsselten Daten verfügt. Eine Prüfung der Daten erfolgt somit bevor diese das KIM-Clientmodul in Richtung Primärsystem oder TI verlassen. Die Funktionalität des KIM Clientmoduls als Anwendungsproxy wird dabei beibehalten, da eine Sicherstellung der Integrität der Datenströme unerlässlich ist.

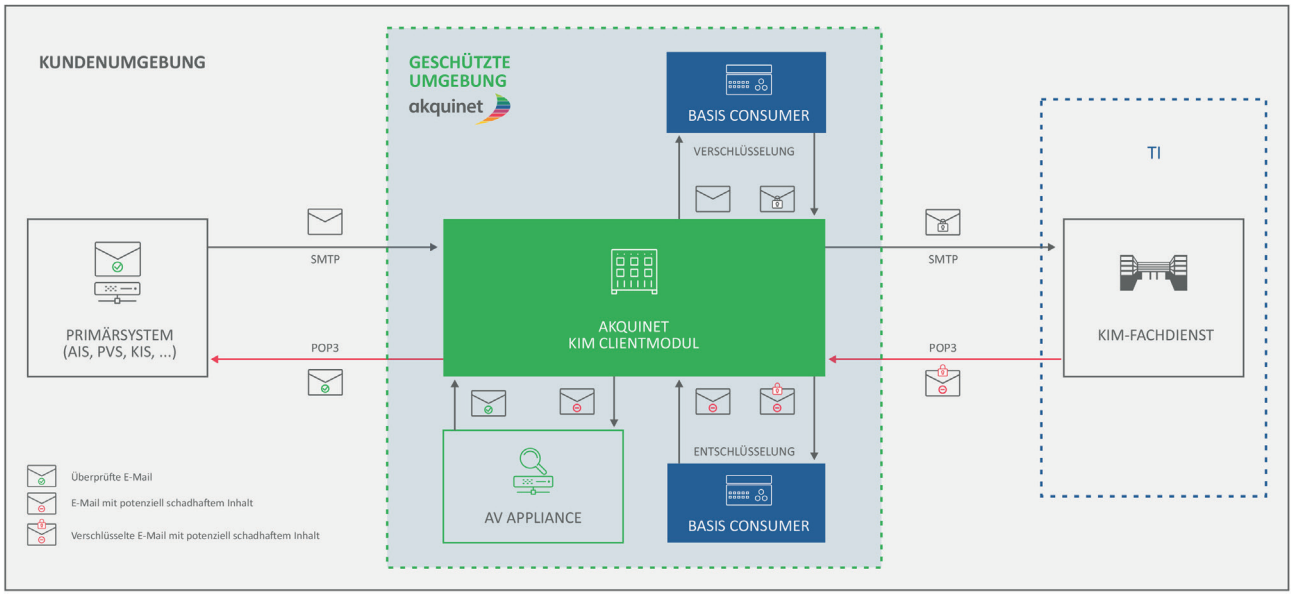
Bei Fund von schadhaftem Inhalt werden dem Anwender die Daten in gesicherter Form, mit Hinweisen zum eigenverantwortlichen Umgang, bereitgestellt. Ein Prüfvermerk in der E-Mail (analog zu den KIM-Vermerken Entschlüsselung & Integritätsprüfung) weist auf den erfolgten Check hin.

Die Architektur

Variante I: Normaler TI-Konnektor



Variante II: „Software Konnektor“ **Basis Consumer (Link)**



Die Funktionsweise

Das KIM Clientmodul übermittelt die E-Mail-Daten an die AntiVirus-Appliance. Dieser Vorgang erfolgt direkt nach der Entschlüsselung der Daten und vor der Weitergabe dieser an das Primärsystem. Die gesamte E-Mail sowie geschachtelte Inhalte werden von der AV-Appliance auf bekannte oder schädlich wirkende Inhalte gescannt. Optional erfolgt eine Prüfung der Daten vor dem Versand über das KIM Clientmodul. Beim Fund potenzieller Schadsoftware werden die Daten in einem passwortgeschützten ZIP-Archiv unter Quarantäne gestellt. Somit wird automatisiertes, versehentliches Entpacken und/oder Ausführen von Schadsoftware vermieden. Auch sämtliche, verschachtelte Anhänge werden unter Quarantäne gestellt. .

Darüber hinaus wird der Prüfvermerk der abgerufenen E-Mail mit Hinweisen versehen. Zur vereinfachten, maschinellen Verarbeitung im Empfängersystem erscheint eine zusätzliche Warnung im E-Mail-Header. Die definierte Funktionsweise des KIM-Clientmoduls als Anwendungsproxy bleibt bestehen.
Der Betrieb der AntiVirus-Appliance findet in einer geschützten Umgebung statt, was die Kontrolle über alle Datenströme ermöglicht. Somit sind eine zentralisierte Verwaltung und Aktualisierung gewährleistet, u.a. durch das tägliche Update der Malware-Datenbank.

Hinweise:

- Die abgebildete Lösung stellt einen zusätzlichen Schutz ohne Gewähr dar. Die Verantwortung zur Prüfung von Daten auf schadhaften Inhalt obliegt final des Primärsystems und jener in dieser Umgebung geltenden Security-Policies.
- Die Nutzung dieser Lösung erfolgt im KIM as a Service (KIMaaS) Angebot der AKQUINET.
- Preis 500,00 EUR im Monat zzgl. MwSt.

Kontakt

Dirk Aagaard
Geschäftsführer Gesundheitswesen

+ 49 (0) 40 88 173 4540
dirk.aagaard@akquinet.de

akquinet

akquinet AG | Paul-Stritter-Weg 5 | D-22297 Hamburg | knowhow@akquinet.de

www.akquinet.com