genua.

Wie eine zweistufige Firewall die Versichertendaten schützt

Die Stuttgarter Lebensversicherung a.G. bietet mit über 100 Jahren Tradition Lösungen für die private Altersvorsorge, Risikoabsicherung und betriebliche Altersvorsorge an. Sie legt besonderen Wert auf finanzielle Solidität, innovative Produkte und konsequente Nähe zum Kunden. Der Schutz der sensiblen Versichertendaten hat hier einen besonders hohen Stellenwert.

Bei der Stuttgarter wird die interne Datenverarbeitung von externen Verbindungen strikt getrennt. Zweistufige Firewalls fungieren als zentrale Schutzkomponente.

von Martin Ortgies, freier Journalist

Security made in Germany

Ein unzureichender Schutz von Kunden- und Versichertendaten kann für Finanzdienstleister und Versicherungen schnell existenzbedrohend werden. Deshalb haben IT-Security-Konzepte einen besonders hohen Stellenwert. Bei der Stuttgarter Lebensversicherung a.G. wird die interne Datenverarbeitung gegen externe Verbindungen strikt abgeschottet. Zweistufige Firewalls übernehmen dabei die Hauptaufgabe.

Projekt-Steckbrief

Der Kunde:
Stuttgarter Lebensversicherungs a.G., Dienstleister für Risikoabsicherung sowie private und betriebliche Altersvorsorge

Die Aufgabe:
Umfassende und performante Inhaltskontrolle an der Schnittstelle Unternehmensnetz-Internet zum Schutz der sensiblen Versichertendaten

Die Lösung:
Einsatz der vom BSI nach CC EAL 4+ zertifizierten und für VS-NfD (Verschlusssachen – nur für den Dienstgebrauch) zugelassenen High Resistance Firewall genugate in einem hochverfügbaren Cluster von genua

Zweistufige Firewalls fungieren als zentrale Torwächter

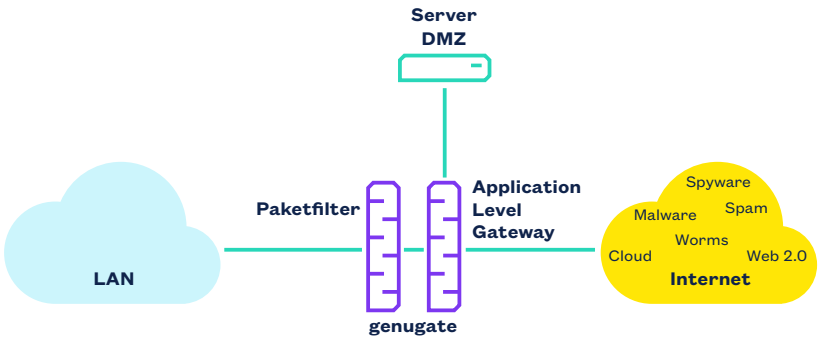
Bei der Stuttgarter wird die interne Datenverarbeitung von externen Verbindungen strikt getrennt. Externe Zugriffe und Verbindungen nach außen werden nur für ausgewählte Transaktionen zugelassen. Zusätzlich sind die Netzsegmente in unterschiedliche Sicherheitszonen aufgeteilt. Als zentrale Torwächter fungieren zweistufige Firewalls. Sie sind die zentrale Schutzkomponente. Auch Virenscans erfolgen zentral an den Firewalls. „In der Standardeinstellung der Firewall lassen wir nach außen keine Verbindungen zu. Notwendige Dienste aus dem Internet werden stark gefiltert. Verbinden dürfen sich nur Anwendungen, die als zwingend notwendig definiert sind, wie ein- und ausgehende E-Mails. Hier wirkt das Graylisting von genugate als effektiver Spamfilter.

Selbst wenn sich ein Mitarbeiter auf verschlungenen Wegen eine Malware-Infektion eingefangen haben sollte, wird die Schadsoftware daran gehindert, eine Verbindung zu einem externen Control Server aufzubauen“, erläutert Siggi Langauf, Head of System Administration bei der Stuttgarter, die Philosophie des Sicherheitskonzepts.

Entscheidung für Firewall genugate

Bei der Firewall als der zentralen Sicherheitskomponente hat sich die Stuttgarter bereits 2003 für „genugate“ von genua entschieden. Der deutsche IT-Sicherheitshersteller genua mit Sitz in Kirchheim bei München ist seit 2015 ein Unternehmen der Bundesdruckerei-Gruppe.

Bei genugate sind zwei Firewall-Systeme zu einer abgestimmten Lösung kombiniert: Ein Application Level Gateway ALG setzt die ankommenden Pakete zu Datensätzen zusammen und analysiert den Inhalt. Gefährliche Daten wie aktiver Content oder Viren werden erkannt und abgeblockt. Zulässige Daten werden über eine neue Verbindung weitergeleitet. Hier liegt der wesentliche Vorteil gegenüber herkömmlichen Firewalls ohne ALG – diese können Schadprogramme, die zunächst als harmlos erscheinende kleine Datenpakete ankommen, oft nicht erkennen. Als zweite Stufe nach dem ALG kontrolliert der Paketfilter (PFL) von genugate die Datenpakete anhand der Header-Informationen wie IP-Adresse, Protokolltyp und Port-Nummer.



Hochsichere Übergänge durch die High Resistance Firewall genugate

Die Firewall als zentrale Sicherheitskomponente

Siggi Langauf hebt als das Besondere an genugate hervor, dass die Regeln dieser klassisch administrierten Firewall nicht durch statistische Methoden oder undurchschaubare Regeln einer künstlichen Intelligenz bestimmt werden: „Für uns ist es entscheidend, dass alle Einstellungen der Firewall transparent sind und dass das Verhalten der Firewall vorhersagbar ist.“ Im Rahmen des Informations-Sicherheits-Managements ISMS werden die Regularien regelmäßig überprüft. Jede Firewall-Regel muss dokumentiert sein und einen Ansprechpartner haben, berichtet der Leiter der Systemadministration.

Als wichtiges Kriterium für eine Firewall nennt er die regelmäßige Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI). Das BSI überprüft von unabhängiger Seite die zuverlässige Sicherheitsleistung sowie den starken Selbstschutz gegen direkte Angriffe. Hier erfüllt genugate die Anforderungen des Sicherheits-Levels EAL 7 – als einzige Firewall der Welt. Auch bei Sicherheitsvorfällen wie dem OpenSSL-Bug „Heartbleed“ oder „Poodle“ war genugate nicht angreifbar.

„Die Firewall hat sich als sehr sicher bewährt. Sie wird ständig auf den neuesten Stand gebracht und es gibt trotz vieler Angriffsversuche keine Schwachstellen. Sie hat uns kein einziges Mal im Stich gelassen“, bestätigt der Leiter der Systemadministration das hohe Sicherheitsniveau.

Beim wichtigen Kriterium Selbstschutz gegen direkte Angriffe erfüllt genugate die Anforderungen von Stufe EAL 7 - als einzige Firewall der Welt.

Zertifizierung und Zulassung durch das Bundesamt für Sicherheit in der Informationstechnik

genugate ist zertifiziert nach dem Standard Common Criteria (CC) in der anspruchsvollen Stufe EAL 4+ und zugelassen für VS-NfD, NATO RESTRICTED und RESTREINT UE/ EU RESTRICTED.

Versicherung stellt hohe Anforderungen an den Hersteller

Für die Stuttgarter ist es sehr wichtig, dass vom Datenverkehr nicht nur Stichproben kontrolliert werden, sondern eine 100-%-Erfassung erfolgt und dabei auch die neuesten Protokolle erkannt werden. Eine Komplettprüfung aller Verbindungen und Dateien erfordert allerdings eine hohe Leistung. genugate kann je nach Anzahl der Nutzer, dem Traffic-Umfang und den Anforderungen des Sicherheitskonzepts flexibel skaliert werden. So stellen mehrere Firewalls im Verbund bei Ausfall einer Komponente die Hochverfügbarkeit (High Availability) sicher und ermöglichen auch bei einem hohen Traffic-Aufkommen eine ausreichende Performance. „Trotz der hohen Sicherheitsleistung erreicht die Firewall einen hohen Datendurchsatz. Nur beim Download sehr großer Dateien wird es etwas langsamer. Das nehmen wir für den Sicherheitsgewinn bewusst in Kauf“, wägt Siggi Langauf ab.

Die Stuttgarter stellt an die Hersteller ihrer Sicherheitskomponenten hohe Anforderungen. Ein deutscher Hersteller gilt aus Sicherheitssicht als vorteilhaft. Außerdem wird eine hohe Kompetenz für den gesamten Netzwerkbereich als Voraussetzung gesehen. Weil sich das gesamte Umfeld sehr schnell verändert, ständig neue Protokolle eingesetzt werden und laufend unbekannte Verbindungsprobleme auftauchen, benötigen Administratoren zuverlässige Unterstützung. Hier ist ein schneller und fachlich kompetenter Support wichtig. Nach den Erfahrungen bei der Stuttgarter sind bei vielen Problemen zunächst nur die Symptome erkennbar. Die Ursachenanalyse erfordere oft sehr großes Fach-Know-how.

Partnerschaftliche Zusammenarbeit

„Wir hatten beispielsweise in der Vergangenheit viele falsch konfigurierte Webserver, wo die SSL-Zertifikate nicht korrekt hinterlegt waren. Die Webseiten wurden von der Firewall standardmäßig abgewiesen. Von genua haben wir einen Workaround erhalten, der eine Verbindung ermöglichte und trotzdem sicher war“, nennt der Leiter der Systemadministration ein Beispiel. Die Zusammenarbeit sei partnerschaftlich. Man werde auch als mittelständisches Unternehmen vom Support ernst genommen.

„Die Firewall genugate wird ständig auf den neuesten Stand gebracht und es gibt trotz vieler Angriffsversuche keine Schwachstellen. Sie hat uns kein einziges Mal im Stich gelassen.“

Siggi Langauf, Head of System Administration, Stuttgarter Lebensversicherung a.G.

Weitere Informationen:

www.genua.de/genugate

1023-07-DE

Über genua

Die genua GmbH ist Enabler der digitalen Transformation. Wir sichern sensible IT-Netzwerke im Public- und im Enterprise-Sektor, bei KRITIS-Organisationen und in der geheimschutzbetreuten Industrie mit hochsicheren und skalierbaren Cyber-Security-Lösungen. Dabei fokussiert sich die genua GmbH auf den umfassenden Schutz von Netzwerken, Kommunikation und interner Netzwerksicherheit für IT und OT. Das Lösungsspektrum umfasst Firewalls & Gateways, VPNs, Fernwartungssysteme, interne Netzwerksicherheit und Cloud Security sowie Remote-Access-Lösungen für mobile Mitarbeiter und Home Offices.

Die genua GmbH ist ein Unternehmen der Bundesdruckerei-Gruppe. Mit mehr als 400 Mitarbeitenden entwickelt und produziert sie IT-Security-Lösungen ausschließlich in Deutschland. Seit der Unternehmensgründung 1992 belegen regelmäßige Zertifizierungen und Zulassungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) den hohen Sicherheits- und Qualitätsanspruch der Produkte. Zu den Kunden zählen u. a. Arvato Systems, BMW, die Bundeswehr, das THW sowie die Würth-Gruppe.

genua GmbH, Domagkstraße 7, 85551 Kirchheim bei München
+49 89 991950-0, info@genua.de, www.genua.de