

Case Study

Deutsche Privatbank

Netzwerksichtbarkeit, die sich rechnet

Wie eine Bank Netzwerkvorfälle schneller erkennt, analysiert und nachhaltig optimiert

Branche: Finanzen

Kunde: Führende deutsche Bank

Herausforderung: Volle Sichtbarkeit bis auf Paketebene – bei Netzwerkproblemen, Anomalien und sicherheitsrelevanten Ereignissen

Bei Problemen im IT-Netzwerk spielt der Faktor Zeit eine entscheidende Rolle. Eine umfassende Transparenz des Netzwerkverkehrs bis auf die Paketebene ist unerlässlich, um im Ernstfall effizient handeln zu können. Eine führende deutsche Bank entschied sich für Allegro Packets, um Daten zuverlässig aufzuzeichnen und relevante Informationen schnell bereitstellen zu können.

Herausforderung: Wenn Sekunden zählen

Der Kunde benötigt eine permanente Aufzeichnung des Netzwerkverkehrs. Aufgezeichnete Probleme und Anomalien sollen innerhalb eines definierten Zeitfensters extrahiert werden, um sie retrospektiv auszuwerten. Es soll schnell erkannt werden, wo Anomalien erstmals auftraten, wie und wohin sie sich in geschäftskritischen Systemen (z. B. Zahlungsverkehr oder Kernbankensysteme) verteilten und ob ein wiederkehrendes Muster zu erkennen ist. Dies soll auf Basis von Rohdaten auf Paketebene erfolgen.

Bisher setzte der Kunde die integrierte Paketaufzeichnung des Herstellers einer Sicherheitslösung ein. Der Einkaufspreis und die laufenden Wartungskosten standen allerdings in keinem wirtschaftlich sinnvollen Verhältnis zum gelieferten Analyseumfang. Darum suchte er nach einer Alternative mit besserem Preis-Leistungsverhältnis anstatt den bestehenden Wartungsvertrag zu verlängern.

Zusammengefasst stand der Kunde vor folgenden Problemen:



- Fehlende Nachvollziehbarkeit von Netzwerkaktivitäten im Finanzdatenverkehr
- Eingeschränkte forensische Analyse bei sicherheitsrelevanten Ereignissen
- Verzögerte Ursachenanalyse bei Störungen geschäftskritischer Systeme (z. B. Zahlungsverkehr, Core Banking)
- Herausforderungen bei der Einhaltung von Compliance- und Audit-Anforderungen
- Großer manueller Aufwand für Ad-hoc-Paketmitschnitte im Incident-Fall
- Hohe Kosten der bestehenden Lösung bei gleichzeitig begrenztem Analyseumfang

Lösung: Mehr Verständnis dank Netzwerktransparenz

Die Bank entschied sich für ein Allegro Network Multimeter 3500, um Netzwerktransparenz auch in zeitkritischen Situationen sicherzustellen. Ein entscheidender Vorteil liegt im integrierten Paketringspeicher: Netzwerkdaten werden kontinuierlich aufgezeichnet und stehen dadurch auch rückwirkend für Analysen zur Verfügung. Das IT-Team kann so jederzeit auf einen definierten Zeitraum in der Vergangenheit zugreifen, ohne aufwendige manuelle Mitschnitte oder vorbereitende Maßnahmen.

Die flexibel skalierbare Speicherarchitektur ermöglicht es, die Aufzeichnung exakt an die Anforderungen der Bank anzupassen. So lassen sich die Daten granular filtern – etwa nach Paketlängen oder spezifischen Datenströmen. Gleichzeitig gewährleisten integrierte Sicherheitsfunktionen wie die AES-256-Verschlüsselung und redundante Speicherung eine jederzeit sichere und auditierbare Datenhaltung.

Das Allegro Network Multimeter integriert sich nahtlos in die bestehende Infrastruktur und kann Daten flexibel erfassen – sei es direkt im Datenpfad, über SPAN-Ports oder standortübergreifend via ERSPAN.

Im Analysefall profitiert das IT-Team von einer intuitiven Auswertung: Relevante Datenflüsse lassen sich visuell aufbereiten und mit wenigen Klicks als Pcap exportieren. Dadurch wird eine detaillierte Untersuchung auf Paketebene erheblich beschleunigt.

Ergebnisse: Weniger Kosten, mehr Planungssicherheit

Mit dem Allegro Network Multimeter konnte die Bank ihre zentrale Anforderung vollständig erfüllen: die zuverlässige Aufzeichnung und schnelle Analyse von Netzwerkdaten unmittelbar vor und nach Anomalien und sicherheitsrelevanten Ereignissen.

Durch den kontinuierlichen Zugriff auf historische Daten ist das IT-Team heute in der Lage, Vorfälle deutlich schneller und präziser zu untersuchen, ohne auf vorbereitende Maßnahmen angewiesen zu sein. Kritische Daten stehen jederzeit zur Verfügung – genau dann, wenn sie benötigt werden.

Auch wirtschaftlich überzeugte die Lösung: Im Vergleich zur Weiterführung der bisherigen Infrastruktur amortisierte sich die Investition bereits nach rund zwei Jahren – bei einer geplanten Nutzungsdauer von fünf Jahren.

Die Bank profitiert damit nicht nur von höherer Transparenz, sondern auch von einer deutlich verbesserten Kostenstruktur und langfristigen Planungssicherheit.

Case Study

Deutsche Privatbank

Die wichtigsten Vorteile im Überblick:



- Revisionssichere Netzwerkforensik durch vollständige Paketaufzeichnung
- Deutlich schnellere Aufklärung von Sicherheitsvorfällen und Anomalien im Finanzdatenverkehr
- Minimierung von Ausfallzeiten geschäftskritischer Anwendungen (z. B. Zahlungsverkehr, Trading)
- Reduziertes Risiko von Compliance-Verstößen und Reputationsschäden
- Optimierte Ressourcennutzung der IT
- Planbare und langfristig optimierte Kostenstruktur

Ausblick und Fazit: Ein Investment, das sich auszahlt

Die Bank verfügt nun über eine leistungsstarke und zukunftssichere Lösung zur Netzwerksichtbarkeit, selbst in hochperformanten Rechenzentrumsumgebungen mit Bandbreiten von bis zu 200 Gbit/s.

Gleichzeitig schafft die Lösung die Grundlage für weiteres Optimierungspotenzial. Zusätzliche Analysefunktionen stehen bereits heute zur Verfügung und können bei Bedarf aktiviert werden, um die Effizienz in der Fehlersuche und Analyse weiter zu steigern.

Die Bank ist damit nicht nur für aktuelle Anforderungen bestens aufgestellt, sondern kann ihre Netzwerkstrategie auch künftig flexibel weiterentwickeln – und schafft damit die Basis für eine zunehmend proaktive statt reaktive Netzwerkanalyse.

Über Allegro Packets

Allegro Packets, ein in Deutschland ansässiges Unternehmen, bietet portable und Rack-Lösungen für die Netzwerkanalyse und die Erfassung von Datenpaketen an. Der Hersteller setzt neue Maßstäbe durch die Kombination von hoher Leistung, Zuverlässigkeit, aktiver Entwicklung, unermüdlichem Support und fairen Preisen mit seinem All-in-One-Angebot. Die Lösungen von Allegro Packets genießen weltweit Anerkennung und werden von Dienstleistern, Regierungsorganisationen, Gesundheitseinrichtungen und Unternehmen eingesetzt.

Website: www.allegro-packets.com