LINK11

CASE STUDY

Quipu
Part of the ProCredit Group

www.link11.com

Case Study Quipu

Sicherheit, die sich der Anwendung anpasst: Wie Quipu mit Link11 eine einzigartige Lösung fand

In der hochsensiblen Welt der Finanztechnologie reichen Standard-Sicherheitslösungen oft nicht aus. Die Quipu GmbH ist das Rückgrat der ProCredit Gruppe. Die Verwendung von Cloud-Schutzmaßnahmen „von der Stange“ hinterließ kritische Lücken in der Verteidigung. Quipu stand vor der Herausforderung, komplexe Web-Angriffe abzuwehren, fand am Markt jedoch nur starre Einheitslösungen. Deshalb suchte das Unternehmen einen Partner, der sich flexibel an ihre spezifische Infrastruktur anpasst.

Der digitale Motor der ProCredit Gruppe

Gegründet im Jahr 2004, fungiert die Quipu GmbH als dedizierter IT-Dienstleister für die ProCredit Gruppe, eine entwicklungsorientierte Geschäftsbankengruppe, die vornehmlich in Osteuropa und Deutschland tätig ist. Mit Hauptsitz in Frankfurt hat sich Quipu von einer reinen Support-Einheit zu einem fortschrittlichen Technologieunternehmen entwickelt, das für den gesamten digitalen Lebenszyklus der Gruppe verantwortlich ist: von der Bankensoftware und Kartenzahlungsdiensten bis hin zu Cloud und Infrastruktur.

Quipus Philosophie konzentriert sich auf „Made-to-fit“-Lösungen. Das Unternehmen entwirft IT-Architekturen, die lokale Marktanforderungen respektieren und gleichzeitig globale Expertise nutzen. Diese interne Mission macht sie besonders sensibel für die Qualität ihrer eigenen Lieferantenbeziehungen: Sie erwarten dasselbe Maß an Anpassungsfähigkeit, das sie auch ihren eigenen Kunden bieten.

Mit einer Strategie, die auf ein vollständig digitales Bankenerlebnis ausgerichtet ist, ist die maximale Verfügbarkeit nicht verhandelbar. Fast alle Kundeninteraktionen finden über das Internet statt, was die Frontend-Services zur Lebensader des täglichen Bankgeschäfts macht. In diesem Umfeld bedeutet Ausfallzeit sofortigen Umsatzverlust und schwindendes Kundenvertrauen.

Wenn cloud-native Schutzmaßnahmen an ihre Grenzen stoßen

Ursprünglich wurden die Frontend-Services von Quipu in der Cloud gehostet und durch die nativen Sicherheitsfunktionen des Providers, einschließlich WAF und Rate-Limiting, geschützt. Das Team ging davon aus, dass dieser Standard-Schutzwall ausreichen würde, um gängige Bedrohungen abzuwehren.

Die Realität sah jedoch anders aus, als es Angreifern gelang, diese Verteidigungslinien mit kleinen Bot-Attacken zu umgehen und kritische Dienste lahmzulegen. Die nativen Tools erwiesen sich als zu ungenau für die erforderliche Präzision. Um Angriffe abzuwehren, wurde das Sicherheitsteam von Quipu in eine reaktive Ecke gedrängt: Sie mussten manuell Rate-Limits senken oder den Datenverkehr aus ganzen Ländern blockieren. Dies stoppte zwar die Bots, sperrte aber auch legitime Kunden aus, womit das Ziel der Angreifer – ein Ausfall des Dienstes – effektiv erreicht war.

Als sich Quipu an ihren Cloud-Provider wandte, um eine dauerhafte Lösung zu finden, war die Antwort alarmierend. „Uns wurde gesagt, es gäbe keine Wunderwaffe“, erklärte Borut Lape, Senior Cybersecurity Officer bei Quipu. Das Team musste folglich jede Komponente der Infrastruktur separat absichern, anstatt auf eine übergreifende Lösung zurückgreifen zu können. Es war ein enormer manueller Aufwand ohne Sicherheitsgarantie.

Der Ausweg aus der „Standard-Falle“

Als Quipu die Anforderungen für eine neue Sicherheitsarchitektur definierte, kristallisierten sich bestimmte Kriterien als essenziell heraus. Faktoren, die letztlich entscheiden würden, welche Anbieter ihre Bedürfnisse realistisch bedienen konnten.

1 Der Bedarf an einem Fully Managed Service

Quipu hatte bereits mit On-Premise-WAF-Appliances experimentiert, kam jedoch zu dem Schluss, dass der operative Aufwand nicht angemessen ist. Die Pflege komplexer Regelsätze erforderte Spezialwissen, das schnell verloren ging, wenn Schlüsselmitarbeiter das Unternehmen verließen. „Wir hatten kein dediziertes Team, um das zu verwalten. Selbst wenn Mitarbeiter geschult sind, aber nicht täglich mit der Lösung arbeiten, ist das Wissen selten auf dem erforderlichen Niveau“, erklärte Borut Lape. Sie benötigten einen Partner, der ihnen diese komplexe Aufgabe abnimmt.

2 Custom Ports als entscheidendes Unterscheidungsmerkmal

Eine kritische technische Anforderung war die Unterstützung von benutzerdefinierten Ports (Custom Ports). Die Umgebung von Quipu nutzte spezifische Ports jenseits der Standards 80 und 443. Obwohl Quipus IT-Architektur valide und funktional war, konnten viele große Hyperscaler dies schlichtweg nicht unterstützen und boten nur starre Standardkonfigurationen an.

3 Compliance & Vertrauen

Als Finanzdienstleister war die strikte Einhaltung von PCI-DSS, DSGVO- und DORA-Vorschriften obligatorisch. Der ideale Partner musste einen authentischen und qualitativen Ansatz für Datenschutz und die Einhaltung gesetzlicher Vorschriften bieten.

Eine einzigartige Lösung in einem starren Markt

Quipu hat mehrere Anbieter am Markt evaluiert. Dabei ist klar geworden: Das Umfeld ist zu unflexibel. Konfrontiert mit komplexen Preisstrukturen und Anbietern, die lieber ihre Standard-Lösungen verkaufen wollten als auf Kundenwünsche einzugehen, fühlte Quipu sich nicht ernst genommen.

Link11 stach heraus, indem sie das anboten, was Sean Power, Solution Engineer bei Link11, als maßgeschneiderte Lösung beschreibt: „Quipu benötigte eine Lösung, die sich anpasst und ihre Anforderungen ergänzt.“ Jenseits dieser technischen Flexibilität zeigte Link11 eine einladende, kundenorientierte Haltung, durch die sich Quipu von Anfang an verstanden und priorisiert fühlte. Anstatt den IT-Dienstleister zu zwingen, seine Anwendung an das Sicherheitstool anzupassen, passte Link11 seinen Schutz an die Realität des Kunden an.

Diese Flexibilität ermöglichte es Quipu, ihre Umgebungen mit Custom Ports zu sichern, ohne ihre gesamte Infrastruktur neu entwickeln zu müssen. Die Lösung von Link11 bestand aus einer soliden Basis von 75 % Standardprodukt, während die verbleibenden 25 % individuell angepasst oder von Grund auf neu entwickelt wurden, um Quipus exakten Bedürfnissen zu entsprechen.

Eine Partnerschaft, basierend auf tief verankertem Vertrauen

Die Entscheidung für Link11 ging über technische Spezifikationen hinaus; sie basierte auf einer bewährten Zuverlässigkeit. Link11 war bereits ein vertrauenswürdiger Partner für Quipu und stellte erfolgreich ISP- und DDoS-Schutzdienste bereit. Die Erweiterung dieser Beziehung auf die kritische Web Application Security war eine logische Evolution, basierend auf transparenter Kommunikation und Stabilität.

„Mit Link11 erhielten wir einen sehr persönlichen Ansatz, eine echte menschliche Beziehung.“

Borut Lape, Sr. Cybersecurity Officer Quipu

Dieses bereits bestehende Vertrauen wurde während der Implementierung der neuen WAAP-Lösung gefestigt. In einer Branche, die oft durch anonyme Support-Warteschleifen geprägt ist, hat Link11 einen Solution Engineer zur Verfügung gestellt, der praktisch zu einer Erweiterung von Quipus internem Team wurde. Dies ging über einfachen Support hinaus – es wurde sichergestellt, dass die spezifischen Nuancen von Quipus Infrastruktur tiefgreifend verstanden und nicht nur oberflächlich für ein einzelnes Ticket erlernt wurden. Borut Lape hebt diesen Kontrast zwischen transaktionsorientierten Anbietern und einem echten Partner hervor: „Mit Link11 erhielten wir einen sehr persönlichen Ansatz, eine echte menschliche Beziehung." Für Quipu bedeutete dies eine direkte Steigerung des Sicherheitsgefühls. Zu wissen, dass die Menschen, die ihre Infrastruktur schützen, genauso in deren Stabilität investiert sind wie sie selbst.

Vom reaktiven „Feuerlöschen" zur proaktiven Resilienz

Der Übergang zu einem Fully Managed Service von Link11 hat die Sicherheitsaufstellung von Quipu grundlegend von reaktiv zu resilient gewandelt.

Operative Freiheit:
Anstatt Ressourcen für manuelle Konfigurationen und potenzielle Gefahrenabwehr aufwenden zu müssen, wird das interne Team durch die Experten von Link11 effektiv von dieser operativen Last befreit.

Vermeidung von Kollateralschäden:
Die Lösung stellt sicher, dass Angriffe bereits in der Cloud abgewehrt werden und das Rechenzentrum von Quipu nie erreichen. Dies verhindert Bandbreitensättigung und Kollateralschäden an anderen Systemen, die typischerweise bei On-Premise-Appliances auftreten.

Strategische Sicherheit:
Weg von der vermeintlichen Sicherheit der Vergangenheit, operiert Quipu nun mit einer Schutzschicht, die aktiv gemanagt und garantiert wird. Dies erlaubt es ihnen, sich auf ihre Kernmission zu konzentrieren: digitale Innovation für den Bankensektor.

Partnerschaft in der Praxis: Langfristige Stabilität sichern

Die Implementierung befindet sich derzeit in einer ausgedehnten Onboarding-Phase. Dies ist eine bewusste Strategie, um Sicherheit und Präzision vor Schnelligkeit zu stellen. Dieser sorgfältige Rollout, unterstützt durch Link11, unterstreicht die Natur der Partnerschaft: Es geht nicht um eine schnelle Lösung, sondern um langfristige Stabilität. Für andere Organisationen, die vor ähnlichen Herausforderungen stehen, hat Borut Lape einen klaren Rat:

„Analysieren Sie Ihre Infrastruktur im Detail und nehmen Sie sich Zeit, die ‚menschliche Seite' der Zusammenarbeit mit dem Provider zu testen, nicht nur die Spezifikationen auf dem Papier."

Borut Lape, Sr. Cybersecurity Officer Quipu

Mit Link11 fand Quipu mehr als nur einen Lieferanten; sie fanden einen Partner, der fähig ist, einen Schutzschild zu bauen, welcher sich ihrem einzigartigen digitalen Fußabdruck anpasst. Ihre Reise markiert einen entscheidenden Übergang von reaktiver Schadensbegrenzung zu einer proaktiven, vollständig gemanagten Sicherheitsstrategie. Sie beweist, dass in der Welt kritischer Infrastrukturen persönlicher Support und maßgeschneidertes Engineering die einen wesentlichen Beitrag zur Sicherheit leisten können. Dieser umfassende Ansatz stellt sicher, dass die Bankdienstleistungen der ProCredit Gruppe für das Geschäft geöffnet bleiben – egal, wie die Bedrohungslage aussieht.

Quipu
Part of the ProCredit Group

Quipu ist ein deutscher IT-Dienstleister, der maßgeschneiderte Lösungen für Banking-Software, Kartenzahlungssysteme und digitale Finanzinfrastruktur entwickelt. Das Unternehmen betreibt ein weltweites Netzwerk sicherer IT-Systeme für Banken und Finanzinstitute, darunter das ProCredit Banken-Network. Quipu ist PCI-DSS-zertifiziert und bietet Zahlungsverkehrslösungen sowie Cloud-Infrastruktur „Made in Germany", die höchste Sicherheits- und Compliance-Standards erfüllen.

LINK11

Link11 ist ein deutscher IT-Sicherheitsanbieter mit Spezialisierung auf DDoS-Schutz und Cyber-Resilienz. Das Unternehmen betreibt ein hochperformantes, KI-gestütztes Schutzsystem, das Angriffe in Echtzeit erkennt und automatisch abwehrt. Link11 ist BSI-zertifiziert, ISO-27001-konform und bietet Sicherheitslösungen „Made in Germany", die weltweit im Einsatz sind.

Link11 GmbH | +49 69 5800492677 | sales@link11.com | www.link11.com