

FALLSTUDIE

Sicredi setzt NIOS DDI und BloxOne Threat Defense ein, um sein Wachstum als führendes Unternehmen im brasilianischen Finanzsektor fortzusetzen



ÜBERSICHT

Sicredi ist ein genossenschaftliches Finanzinstitut, das vor über 120 Jahren gegründet wurde. In den letzten zwei Jahrzehnten hat das Unternehmen eine interne Umstrukturierung durchlaufen und seine Expansion beschleunigt. Um dieses Wachstum zu unterstützen und Innovationen im Finanzsektor voranzutreiben, hat Sicredi in die digitale Transformation investiert.

Kreditgenossenschaften bieten dieselben Finanzprodukte und -dienstleistungen wie traditionelle Finanzinstitute (Girokonten, Karten, Anlagen), unterscheiden sich jedoch hauptsächlich durch ihr Geschäftsmodell. Im Gegensatz zu herkömmlichen Instituten sind bei Kreditgenossenschaften die Mitglieder die tatsächlichen Eigentümer des Unternehmens.

Um dieses Geschäftsmodell erfolgreich umzusetzen, verfolgt Sicredi eine Managementstrategie, die auf die Mitwirkung seiner mehr als sieben Millionen Mitglieder setzt, welche die Rolle der Geschäftsinhaber übernehmen. Mit über 2.500 Filialen ist diese genossenschaftliche Finanzinstitution in allen brasilianischen Bundesstaaten und im Bundesdistrikt vertreten und bietet eine umfassende Palette an finanziellen und nichtfinanziellen Lösungen an.

DIE SITUATION

Geografische Expansion und Digitalisierung treiben das Geschäft der Kreditgenossenschaften voran

Sicredi ist in Bezug auf die Anzahl seiner Filialen und Mitglieder erheblich gewachsen und hat sich in den letzten Jahren zu einem der wichtigsten Akteure im brasilianischen Finanzsektor entwickelt. Derzeit bietet das Unternehmen mehr als 300 Finanzprodukte und -dienstleistungen an, darunter Girokonten und Karten, Investitionen, Versicherungen, Konsortien, Kartengeräte und vollständig digitale Konten für Privatpersonen, Unternehmen und landwirtschaftliche Erzeuger.

“ Infoblox hat die Bereitstellung unserer Produkte für Mitarbeiter und Endnutzer beschleunigt. Früher dauerte die Bereitstellung einer Maschine durchschnittlich fünf Tage. Heute benötigen wir dafür nur noch 15 Minuten. Das System ist flexibler und agiler.

Juliano Luz,
Infrastruktur-Analyst, Sicredi

Um diesen Fortschritt zu begleiten, begann Sicredi 2017 einen Prozess der digitalen Transformation mit dem Ziel, alte Systeme für die Verarbeitung von Produkten und Dienstleistungen (das sogenannte Kernbankgeschäft) schrittweise durch eine modernere Plattform zu ersetzen. Der Einsatz modernster Technologie war entscheidend, um den Mitarbeitern ein besseres Erlebnis zu bieten und die Wettbewerbsfähigkeit auf dem dynamischen Finanzmarkt Brasiliens zu erhalten.

Viele Jahre lang arbeitete Sicredi mit einer technologischen Infrastruktur und virtuellen Maschinen auf „Open Source“-DHCP- und Linux-Tools. Der Infrastrukturanalyst Juliano Luz, der 2008 zu Sicredi kam, erinnert sich an eine veraltete Umgebung: „Es gab Herausforderungen in Bezug auf mangelnde Skalierbarkeit und Agilität. Das Unternehmen benötigte eine neue Anwendung, eine neue Umgebung“, erklärt er.

Da die alte Umgebung mit Open-Source-Lösungen betrieben wurde, gab es keinen externen Support, sodass alle Probleme intern gelöst werden mussten. Und das wiederum erforderte einen hohen Aufwand seitens der IT-Abteilung. Ein weiteres Anliegen von Sicredi war die Verbesserung des Schutzes vor Cyberangriffen.

Sicredi hatte bereits 2013 eine Infoblox-Lösung implementiert, entschied sich jedoch 2021 für eine Aktualisierung der technologischen Umgebung. „Die erste Implementierung von DDI wurde vom internen Team durchgeführt. NTT kam als Partner hinzu, als wir Infoblox NIOS DDI erweiterten und aktualisierten“, so Luz.

DIE HERAUSFORDERUNG

Veraltete technologische Infrastruktur verursacht langsame manuelle Prozesse

Die wachsende Zahl der Finanzprojekte, Dienstleistungen und Produkte von Sicredi erforderte ein Umfeld mit größerer Ausfallsicherheit und Skalierbarkeit. Die veraltete Technologie schränkte die Wachstumspläne des Unternehmens ein. „Unser altes System wurde zu einem Engpass. Die Zuweisung von IP-Adressen und die Erstellung von Datensätzen in einem IP-Adressmanager im DNS-Namen waren sehr langsam“, so Luz. „Die Reservierung der IP-Adressen und die Registrierung der Namen waren kompliziert, was zu einem Mangel an Kontrolle über die Adressierung und zu Problemen mit der Infrastruktur führte.“

Die Infrastruktur erforderte beispielsweise eine höhere Verfügbarkeit der DNS-Server, damit Dateien automatisch und ohne manuellen Aufwand auf einem anderen Rechner repliziert werden konnten. Das IT-Team wollte außerdem den Prozess der Projektaktivierung vereinfachen und beschleunigen, um die Infrastruktur- und Netzwerkteams von diesen Aufgaben zu entlasten. „Zuvor musste ich mich an das Netzwerkteam wenden, um eine IP-Adresse und einen Namen zu erhalten, und dann im letzten Schritt einige Regeln festlegen. Anschließend wurde eine virtuelle Maschine erstellt und auf dem Betriebssystem installiert. All das war sehr langsam“, so Luz.

Die neue Lösung musste auch den Schutz der Mitarbeiter und Geschäftspartner gewährleisten, da Cyberangriffe und digitaler Betrug immer schwerwiegender und häufiger wurden. Darüber hinaus wurden die regulatorischen Rahmenbedingungen strenger, da die brasilianische Zentralbank zunehmend strengere kybernetische Sicherheitskontrollen und -systeme in Finanzinstituten forderte.

Kunde: Sicredi Bank
Branche: Bankwesen
Standort: Brasilien

INITIATIVEN:

- Schaffung einer Umgebung mit größerer Kontingenz und Skalierbarkeit für die wachsende Anzahl von Projekten, Finanzdienstleistungen und Produkten von Sicredi
- Ersatz veralteter Technologieprodukte, die Wachstumspläne einschränkten
- Erhöhung der Verfügbarkeit der Infrastruktur, beispielsweise der DNS-Server, um Dateien automatisch und nicht manuell auf einen anderen Rechner zu replizieren

ERGEBNISSE:

- Verbesserte Qualität und Agilität bei der Bereitstellung von Ressourcen für das Unternehmen
- Beschleunigte die Lieferung von Produkten an Mitglieder und Endbenutzer
- Verbesserte Bereitstellungszeiten: Früher dauerte die Bereitstellung einer Maschine im Durchschnitt fünf Tage; heute kann dies in 15 Minuten erfolgen

LÖSUNGEN:

- NIOS DDI
- BloxOne® Threat Defense

DIE LÖSUNG

Vereinfachte DNS-Verwaltung und verbesserte Sicherheit gegen Cyberangriffe

Sicredi begann mit der Implementierung von Infoblox NIOS DDI, das die grundlegenden Netzwerkdienste von Infoblox unterstützt und einen kontinuierlichen Betrieb der Infrastruktur ermöglicht. Die Implementierung erfolgte in Zusammenarbeit mit dem Partner NTT. Zunächst migrierte Sicredi die DNS-Basis auf die neue Infoblox-Infrastruktur. Im weiteren Verlauf wurden die Funktionen intern und extern erweitert. Infoblox NIOS ermöglichte die Integration und Zentralisierung der DDI-Dienste (DNS, DHCP und IPAM) von Sicredi auf einer einzigen Plattform.

„Neben VMware erfolgte eine Integration mit Infoblox, und all dies wurde automatisiert. Heute können wir auf ein Portal zugreifen, einen Rechner bestellen, den IP-Namen registrieren und die IP reservieren. Anschließend wird ein Betriebssystem installiert und eine VM bereitgestellt, die sofort einsatzbereit ist“, erläutert Andrius Lima, Infrastructure Analyst bei Sicredi. Infoblox ermöglichte außerdem die Automatisierung über APIs, um den Zugriff durch Anwendungen anderer Teams zu erleichtern. Diese Funktionalität war für die wegweisenden Maßnahmen von Sicredi im Rahmen der Programme „Open Banking“ und „Open Finance“ in Brasilien von entscheidender Bedeutung.

Infoblox NIOS hat die Sicherheit, Kontrolle und Transparenz verbessert. Im Jahr 2021 investierte Sicredi in BloxOne Threat Defense, die hybride Sicherheitslösung von Infoblox. Durch diese Implementierung konnte das Unternehmen sein DNS, Datensätze und Kontrollen besser organisieren und von einer insgesamt verbesserten Sicherheitslage profitieren. Dieses Tool ergänzt die Funktionen der bisherigen Umgebung, wie Firewall und DDR.

„Mit Infoblox konnten wir unsere DNS- und DHCP-Infrastruktur skalieren und unsere Umgebung so organisieren, dass sie dem Wachstum des Unternehmens gerecht wird“, erklärt Luz.

DAS ERGEBNIS

Infoblox senkte die Betriebskosten und vereinfachte die Geschäftsabläufe für Sicredi

Der Umstieg auf Infoblox-Lösungen stellte für Sicredi einen enormen Gewinn hinsichtlich der Qualität und Flexibilität bei der Bereitstellung von Ressourcen für das Unternehmen dar. Die neue Infrastruktur senkte die Betriebskosten, da Aufgaben der Netzwerkadministration nun über eine einzige Schnittstelle verwaltet werden und wichtige Prozesse, die zuvor manuell im Rechenzentrum durchgeführt werden mussten, automatisiert und dezentralisiert wurden. Die Genossenschaften können nun ihre eigenen Ressourcen mit Hilfe eines Warteschlangenmanagements verwalten.

„Infoblox hat die Bereitstellung unserer Produkte für Mitarbeiter und Endnutzer beschleunigt. Früher dauerte die Bereitstellung einer Maschine durchschnittlich fünf Tage. Heute benötigen wir dafür nur noch 15 Minuten. Das System ist flexibler und agiler“, erklärt Luz.

Die höhere Verfügbarkeit der Infrastruktur ermöglicht die Verteilung der Dienste auf die beiden Rechenzentren und macht zwingende Eingriffe ohne Unterbrechung des Dienstes erforderlich.

„Aus Gründen der Compliance und Geschäftskontinuität führen wir regelmäßig Tests durch. Mit Infoblox können wir diese Tests mit der Gewissheit vornehmen, dass sie keine Auswirkungen auf den Betrieb von Sicredi haben“, erklärt Luz.

Im Bereich der kybernetischen Sicherheit hat Sicredi Maßnahmen zum Schutz vor Malware- und Ransomware-Angriffen ergriffen und das DoS-Schutztool BloxOne Threat Defense implementiert. Der Manager erklärt, dass Sicredi ohne die Infoblox-Lösungen heute nicht mehr denkbar sei: „Bei Sicredi gilt Infoblox als Teil der Basisdienstleistungen. Der Verlust von NIOS DDI hätte finanzielle und imagebezogene Auswirkungen. Es ist ein unverzichtbares Tool für den Geschäftsbetrieb“, so Luz.

In naher Zukunft plant Sicredi die Integration von Infoblox Cloud DNS, den Erwerb einer Lizenz für Threat Analytics und die Erweiterung der Sicherheitsfunktionen.



Infoblox vereint Netzwerk- und Sicherheitslösungen für ein unübertroffenes Maß an Leistung und Schutz. Wir bieten Echtzeit-Transparenz und Kontrolle darüber, wer und was sich mit Ihrem Netzwerk verbindet, damit Ihr Unternehmen schneller arbeiten und Bedrohungen früher stoppen kann. Darauf vertrauen Fortune-100-Unternehmen und aufstrebende Innovatoren.

Firmenhauptsitz
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054, USA

+1 408 986 4000
www.infoblox.com