The bridge to possible

Cisco Financial Services: Innovative Lösungsansätze

Sicherheit und Widerstandsfähigkeit in Finanzdienstleistungsunternehmen

© 2023 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

The bridge to possible

Sicherheit und Widerstandsfähigkeit in Finanzdienstleistungsunternehmen

Die Widerstandsfähigkeit der Finanzdienstleistungsinfrastruktur ist entscheidend für das Funktionieren der globalen Volkswirtschaften. Risikomanagement war noch nie so wichtig wie heute, denn die externen und internen Faktoren, die sich auf die Finanzdienstleistungsinfrastruktur auswirken, werden immer zahlreicher und dringender. In den letzten 20 Jahren hat die Branche noch nie dagewesene und unvorhersehbare Ereignisse verzeichnet, die zu erheblichen Kredit-, Markt- und Betriebsrisiken geführt haben.

Finanzinstitute von heute benötigen ein widerstandsfähigeres Betriebsmodell, das in der Lage ist, Risiken im großen Stil zu reduzieren und das Unternehmen inmitten unvorhersehbarer Veränderungen zu schützen. Dadurch müssen Institutionen neue Cyberrisiken im Zusammenhang mit der digitalen Expansion von Finanzdienstleistungen, einer zunehmend verteilten Belegschaft und der Nutzung der Cloud zur Differenzierung im Wettbewerb bewältigen.

Die Gesetzeslandschaft im Wandel

Cyberrisiken sind das größte und am schnellsten wachsende Betriebsrisiko im Bereich Finanzdienstleistungen – einer Branche, auf die es Cyberkriminelle seit jeher stark abgesehen haben. Die erheblichen Auswirkungen eines Datenschutzverstoßes haben dafür gesorgt, dass bei Finanzdienstleistern die Cybersicherheitskompetenz, das Schutzniveau und die Ausrichtung auf Normen wie die ISO 27000-Reihe zu IT-Risiken und das Cyber Security Framework des US National Institute of Standards and Technology (NIST) besonders ausgeprägt sind.

Vor Kurzem haben die Regulierungsbehörden auf die zunehmenden Cyberrisiken mit aktualisierten Leitlinien für Institutionen und AuditorInnen reagiert. Der FFIEC hat für US-amerikanische Banken eine Aktualisierung des Architecture, Infrastructure, and Operations Examinations Handbook (Handbuch für Architektur, Infrastruktur und Betriebsprüfungen) sowie der Leitlinien für die Authentifizierung und den Zugriff auf Services und Systeme von Finanzinstituten veröffentlicht. Diese Aktualisierungen sollten die wachsenden Risiken im Zusammenhang mit digitalen Finanzdienstleistungsfunktionen wie Zugriff, Authentifizierung, Cloud-Computing und von Drittanbietern bereitgestellten Services berücksichtigen. Im Vereinigten Königreich hat die Financial Conduct Authority (FCA) im Vorgriff auf zukünftige regulatorische Audits erste Leitlinien für Institutionen, die Remote- oder Hybridarbeit in Betracht ziehen, herausgegeben. Auf der ganzen Welt ergreifen Regulierungsbehörden und Zentralbanken ähnliche Maßnahmen.

Der FFIEC

Der Federal Financial Institutions Examination Council (FFIEC) ist eine formelle behördenübergreifende Einrichtung der US-Regierung, die befugt ist, einheitliche Grundsätze, Standards und Berichtsformulare für die Prüfung von Finanzinstituten auf Bundesebene vorzuschreiben. Er hat das weit verbreitete Cybersecurity Assessment Tool entwickelt, um Finanzinstitutionen bei der Bewertung ihrer Cybersicherheitsbereitschaft zu unterstützen.

Cisco bietet folgende Ressourcen zu FFIEC-Tools an:

- Einführung in die FFIEC-Vorschriften
- FFIEC Cybersecurity Maturity Assessment Tool (Tool zur Bewertung der Cybersecurity-Reife)
- Architecture, Infrastructure, and Operations Examinations Handbook (Handbuch für Architektur, Infrastruktur und Betriebsprüfungen) des FFIEC

© 2023 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

Das Financial Services Information Sharing and Analysis Center (FS-ISAC), ein Branchenkonsortium aus 7.000 Finanzinstituten, erwartet, dass die Cyberbedrohungsaktivitäten zunehmen werden, da Cyberkriminelle verstärkt nach Zero-Day-Schwachstellen suchen.

Social Engineering, Malware und DDoS-Angriffe (Distributed Denial of Service) sind die häufigsten persistenten Bedrohungen in der gesamten Branche. Die Vorhersagen des FS-ISAC für 2022 und darüber hinaus verdeutlichen die Herausforderungen für Finanzinstitute durch Cyberbedrohungen:

- Nationalstaatliche Cyberkampagnen werden geopolitische Spannungen widerspiegeln
- Nationalstaaten werden Lieferketten im Bereich Finanzdienstleistungen beeinflussen
- Ransomware-Gruppen werden sich weiter professionalisieren
- Drittanbieterrisiken stellen eine fortwährende Bedrohung für Finanzunternehmen dar
- Zero-Day-Schwachstellen werden zunehmen
- Regulierungsbehörden werden strengere Vorgaben erlassen
- Die Incident Response wird ausgereifter

Digitalisierung und zunehmende Komplexität

Die Beschleunigung der Digitalisierung hat das Bewusstsein für damit verbundene schnelle IT-Veränderungen und die zunehmende Komplexität geschärft. Dies ist laut dem Deloitte Center for Financial Services und FS-ISAC die größte Cybersicherheitsherausforderung für Finanzinstitute. Die zunehmende Nutzung von Clouds, Datenanalysen und KI/ML bei der Entwicklung neuer Produkte und Services sowie die Notwendigkeit, Remote- und Hybrid-Arbeitsumgebungen zu unterstützen, haben den Umfang und die Skalierung der zu schützenden Elemente erweitert.

IT- und Betriebsverantwortliche konzentrieren sich auf „Security by Design“-Ansätze, um diese wachsenden Herausforderungen zu bewältigen und die zunehmende Komplexität bei der Orchestrierung der Sicherheit über viele unterschiedliche Security-Lösungen hinweg zu reduzieren. SicherheitsexpertInnen benötigen Funktionen, die sich über eine Institution hinweg skalieren lassen und eine umfassende, integrierte und verwaltbare Lösung bieten. Das Ziel besteht darin, die Sicherheitstransparenz zu erhöhen, Entwicklungen vorauszusehen, die richtigen Maßnahmen zu ergreifen und Investitionen in die Widerstandsfähigkeit der gesamten Institution zu stärken.

Die Beschleunigung der Digitalisierung erhöht die Komplexität

© 2023 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten.

Absicherung von Finanzunternehmen

Das Cisco® Secure-Portfolio bietet erstklassige Sicherheit vom Cloud-Edge über Netzwerke, Anwendungen und Workloads bis hin zu EndbenutzerInnen und Geräten.

- Cisco Secure XDR bietet erweiterte Erkennungs- und Reaktionsfunktionen (Extended Detection and Response, XDR), die Sicherheitsteams bei der Erfassung, Untersuchung und Beseitigung von Bedrohungen unterstützen.
- Cisco Secure Connectivity bietet SASE-Funktionen (Secure Access Service Edge) und kombiniert Netzwerk- und Sicherheitsfunktionen in der Cloud, um nahtlosen, sicheren Zugriff auf Anwendungen bereitzustellen – unabhängig davon, wo BenutzerInnen arbeiten.
- Cisco Zero Trust bietet eine umfassende Lösung zum Schutz des Zugriffs auf alle Ihre Anwendungen und Umgebungen durch sämtliche BenutzerInnen, über jegliche Geräte und von jedem Standort aus.
- Cisco Secure Firewall erleichtert Ihnen die Planung und Prioritätensetzung, das Schließen von Lücken sowie die noch stärkere Wiederherstellung nach einem Vorfall. Da MitarbeiterInnen, Daten und Bürostandorte heute überall verteilt sind, muss Ihre Firewall auf alles vorbereitet sein.

Partnerschaften

Auch wenn Cyberrisiken weiterhin Herausforderungen darstellen, sind Finanzinstitute gut aufgestellt, um sie gemeinsam mit anderen Unternehmen der Branche, Aufsichtsbehörden und Anbietern von Sicherheitslösungen wie Cisco zu bewältigen.

Weitere Informationen

Wenn Sie mehr über Finanzdienstleistungen und Technologie erfahren möchten, besuchen Sie Cisco für Finanzdienstleistungen. Weitere Informationen über Security Resilience finden Sie auf unserer entsprechenden Seite.

© 2023 Cisco und/oder Partnerunternehmen. Alle Rechte vorbehalten. Cisco und das Cisco Logo sind Marken oder eingetragene Marken von Cisco und/oder Partnerunternehmen in den Vereinigten Staaten und anderen Ländern. Eine Liste der Marken von Cisco finden Sie unter: www.cisco.com/go/trademarks. Die genannten Marken anderer Anbieter sind Eigentum der jeweiligen Inhaber. Die Verwendung des Begriffs „Partner“ impliziert keine gesellschaftsrechtliche Beziehung zwischen Cisco und anderen Unternehmen. (1110R)

C11-3578322-00 04/23