Leadership éclairé de Cisco en matière de services financiers

La protection d’une entreprise de services financiers résiliente

Contents

La protection d'une entreprise de services financiers résiliente

La résilience des infrastructures de services financiers est essentielle au fonctionnement des économies mondiales. De ce fait, la gestion des risques n'a jamais été aussi importante, car les facteurs externes et internes ayant une incidence sur l'infrastructure des services financiers ont pris de l'ampleur et de la vitesse. Au cours des 20 dernières années, le secteur a traversé des événements imprévisibles sans précédent qui ont créé d'importants risques de crédit, de marché et d'exploitation.

Les institutions financières d'aujourd'hui ont besoin d'un modèle d'exploitation plus résilient, capable de réduire les risques à grande échelle et de protéger l'entreprise dans un contexte de changements imprévisibles. Cela obligera les institutions à gérer les nouveaux risques informatiques associés à l'expansion numérique des services financiers, à une main-d'œuvre de plus en plus décentralisée et à l'utilisation du nuage pour se démarquer de la concurrence.

Un paysage réglementaire en pleine évolution

Le risque cybernétique est le risque opérationnel le plus important et celui qui connaît la croissance la plus rapide dans les services financiers, qui ont la particularité d'être l'un des secteurs les plus ciblés par les cybercriminels. Les conséquences importantes d'une violation de données ont obligé les services financiers à assurer un niveau élevé de compétence en matière de cybersécurité, de protection et d'alignement avec les normes telles que la série 27000 de l'Organisation internationale de normalisation (ISO) sur les risques informatiques et le cadre de cybersécurité du National Institute of Standards and Technology (NIST) des États-Unis.

Récemment, les organismes de réglementation ont réagi à l'augmentation des risques informatiques en mettant à jour des directives à l'intention des établissements et des auditeurs. La FFIEC a notamment publié une mise à jour à l'intention des banques américaines du Architecture, Infrastructure, and Operations Examinations Handbook (manuel d'examens de l'architecture, de l'infrastructure et des opérations), ainsi que des directives sur Authentication and Access to Financial Institution Services and Systems (authentification et l'accès aux services et systèmes des institutions financières). Ces mises à jour visaient à faire face aux risques croissants liés aux capacités des services financiers numériques, ce qui inclut l'accès, l'authentification, l'informatique en nuage et les services fournis par des tiers. Au Royaume-Uni, la Financial Conduct Authority (FCA) a publié des directives initiales à l'intention des établissements qui envisagent le travail à distance ou hybride avant les futurs audits réglementaires. Les organismes de réglementation et les banques centrales adoptent actuellement des mesures similaires partout dans le monde.

Le Financial Services Sharing and Analysis Center (FS-ISAC), un consortium de 7 000 institutions financières, s'attend à ce que les cybermenaces augmentent à mesure que les cybercriminels seront à la recherche de vulnérabilités de jour zéro.

L'ingénierie sociale, les logiciels malveillants et les attaques par déni de service distribué (DDoS) sont les menaces persistantes les plus courantes dans le secteur. Les prévisions du FS-ISAC pour 2022 et au-delà traduisent le difficile environnement de risque cybernétique dans lequel doivent œuvrer les institutions financières :

- Les cybercampagnes étatiques refléteront les tensions géopolitiques.
- Les États-nations influenceront la chaîne logistique des services financiers.
- Les groupes de rançongiciels continueront de devenir de plus en plus professionnels.
- Les risques liés aux tiers continueront de menacer les entreprises offrant des services financiers.
- Les vulnérabilités de jour zéro augmenteront.

- Les organismes de réglementation vont serrer la bride.
- La gestion des incidents gagnera en maturité.

La numérisation et la complexité croissante

L'accélération du numérique a accru la sensibilisation aux changements rapides dans les TI et à leur complexité croissante. Selon le Deloitte Center for Financial Services et le FS-ISAC, il s'agit là du principal défi en matière de cybersécurité que doivent relever les institutions financières. L'utilisation croissante du nuage, de l'analyse des données, de l'intelligence artificielle et de l'apprentissage automatique dans le développement de nouveaux produits et services, ainsi que la nécessité de prendre en charge les environnements de travail à distance et hybrides, ont élargi la portée et le champ de ce qui doit être protégé.

Les responsables des TI et des risques opérationnels se concentrent sur les approches de « sécurité dès la conception » pour gérer cette empreinte croissante et réduire la complexité croissante de l'orchestration de la sécurité sur de nombreuses solutions de sécurité disparates. Les professionnels de la sécurité ont besoin de capacités qui peuvent évoluer dans l'ensemble de l'établissement et offrir une solution complète, intégrée et gérable. L'objectif est d'augmenter la visibilité de la sécurité, d'anticiper la prochaine étape, de prendre les bonnes mesures et de renforcer les investissements dans la résilience de la sécurité à l'échelle de l'établissement.

La protection de l'entreprise financière

La gamme Cisco® Secure offre une sécurité de classe mondiale de la périphérie du nuage aux utilisateurs finaux et aux appareils en passant par les réseaux, les applications et les charges de travail.

- Cisco Secure XDR offre des fonctionnalités de détection et de réponse étendues (XDR) qui fournissent une visibilité et des renseignements exploitables pour aider les équipes de sécurité à repérer les menaces, à enquêter sur celles-ci et à y remédier.
- La connectivité Cisco Secure fournit des capacités de service d'accès sécurisé en périphérie (SASE), et combine les fonctionnalités de réseautique et de sécurité en nuage pour offrir un accès transparent et sécuritaire aux applications, peu importe où se trouvent les utilisateurs.
- Cisco Zero Trust offre une solution complète pour sécuriser les accès aux applications et à l'environnement, peu importe l'utilisateur, l'appareil et le lieu.
- Cisco Secure Firewall renforce vos capacités à planifier, à hiérarchiser et à combler les lacunes, pour ensuite rétablir vos activités. Maintenant que les employés, les données, les succursales et les bureaux sont partout, votre pare-feu doit être prêt à tout.

L'importance des partenaires

Bien que les cyberrisques continuent de poser des défis, les institutions financières sont bien placées pour les gérer en partenariat avec leurs homologues du secteur, les organismes de réglementation et les fournisseurs de solutions de sécurité comme Cisco.

Le FFIEC

Le Federal Financial Institutions Examination Council (FFIEC) est un organisme interagences officiel du gouvernement américain habilité à prescrire des principes, des normes et des formulaires de rapport uniformes pour l'examen fédéral des institutions financières. Il a créé le Cybersecurity Assessment Tool qui est un outil d'évaluation de la cybersécurité largement utilisé pour aider les établissements financiers à évaluer leur état de préparation à la cybersécurité.

Cisco offre l'aperçu suivant des outils du FFIEC.

An introduction to Understanding FFIEC Regulations (une introduction à la compréhension des règlements du FFIEC)

FFIEC Cybersecurity Maturity Assessment Tool (outil d'évaluation de la maturité de la cybersécurité du FFIEC)

The FFIEC's Architecture, Infrastructure, and Operations book (le manuel d'architecture, d'infrastructure et d'exploitation du FFIEC)

L'accélération et l'adoption rapides du numérique augmentent la complexité

Pour en savoir plus

Pour en savoir plus sur les services financiers et les différentes technologies, consultez Cisco dans le secteur des services financiers, et pour en savoir plus sur la résilience de sécurité, consultez notre page sur la résilience de la sécurité.

Siège social aux États-Unis	Siège social en Asie-Pacifique	Siège social en Europe
Cisco Systems, Inc. San Jose. CA	Cisco Systems (USA) Pad Ltd. Singapour	Cisco Systems International BV Amsterdam, Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de télécopieur sont répertoriés sur le site Web de Cisco, à l'adresse **www.cisco.com/go/offices**.

Imprimé aux États-Unis C11-3578322-00 04/23