Livre blanc
Document public de Cisco

The bridge to possible

Les conseils de Cisco pour le secteur des services financiers

Renforcer la résilience des systèmes de sécurité de l'entreprise

The bridge to possible

Renforcer la résilience des systèmes de sécurité de l'entreprise

La résilience de l'infrastructure des services financiers est essentielle au bon fonctionnement des économies mondiales. La gestion des risques n'a jamais été aussi importante, car les facteurs externes et internes qui affectent ces infrastructures ont gagné en ampleur et en rapidité. Au cours des 20 dernières années, le secteur a traversé des événements imprévisibles et inédits qui ont créé d'importants risques au niveau financier, opérationnel et du marché.

Les institutions financières modernes ont besoin d'un modèle d'exploitation plus résilient, capable de réduire les risques à grande échelle et de protéger l'entreprise face aux imprévus. Elles devront donc faire face à de nouveaux risques informatiques associés à l'expansion numérique des services financiers, à la décentralisation de plus en plus forte des effectifs et à l'utilisation du cloud pour se démarquer de la concurrence.

Un cadre réglementaire en mutation

Dans les services financiers, le risque informatique est à la fois le risque opérationnel le plus important et celui qui connaît la plus forte croissance. Le secteur a la particularité d'être l'un des domaines les plus ciblés par les cybercriminels. Les lourdes répercussions en cas de violation de données ont conduit les services financiers à se doter d'un niveau élevé de compétence, de protection et d'alignement sur les normes en matière de cybersécurité, telles que la suite 27000 de l'Organisation internationale de normalisation (ISO) sur les risques IT 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 liés aux cyberattaques en mettant à jour leurs directives à l'intention des institutions et des auditeurs. Le FFIEC, autorité des marchés financiers pour les banques américaines, a publié une mise à jour du Guide sur les contrôles de l'architecture, de l'infrastructure et des opérations, ainsi que des directives pour l'authentification et l'accès aux services et systèmes des institutions financières. L'objectif de ces mises à jour est de faire face aux risques croissants liés aux fonctionnalités numériques des services financiers, notamment l'accès, l'authentification, le cloud computing et les services fournis par des tiers. Au Royaume-Uni, la Financial Conduct Authority (FCA) a publié des directives élémentaires à l'intention des établissements qui envisagent le travail à distance ou hybride avant les prochains audits réglementaires. Des organismes de réglementation et des banques centrales du monde entier prennent des mesures similaires.

Le FFIEC

Le Federal Financial Institutions Examination Council (FFIEC) est un organisme officiel du gouvernement américain qui réunit différentes agences habilitées à édicter ensemble des principes, des normes et des rapports pour le contrôle au niveau fédéral des institutions financières. Il a créé un outil d'évaluation de la cybersécurité largement utilisé pour aider les institutions financières à évaluer leur niveau de préparation en matière de cybersécurité.

Cisco propose les présentations suivantes des outils du FFIEC.

- Présentation des réglementations du FFIEC
- Outil d'évaluation du FFIEC du niveau de maturité en matière de cybersécurité
- Livre du FFIEC sur l'architecture, l'infrastructure et les opérations

Le FS-ISAC (Financial Services Information Sharing and Analysis Center), un consortium de 7 000 établissements financiers, prévoit une augmentation des cybermenaces à mesure que les cybercriminels recherchent des vulnérabilités de type « zero-day ».

L'ingénierie sociale, les malwares 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 dépeignent les risques liés à la cybersécurité auxquels seront confrontées les institutions financières :

- Les campagnes de cybersécurité émanant d'États refléteront les tensions géopolitiques
- Les États influenceront la chaîne d'approvisionnement des services financiers
- Les groupes de ransomwares continueront de se professionnaliser
- Les risques liés aux tiers continueront de menacer les établissements financiers
- Les vulnérabilités zero-day augmenteront
- Les organismes de réglementation renforceront les règles
- Les réponses aux incidents progresseront

La numérisation s'accompagne d'une complexité croissante

L'accélération de la transformation numérique a renforcé la prise de conscience des changements rapides et de la complexité croissante qui y sont associés. Selon le Deloitte Center for Financial Services et le FS-ISAC, c'est le principal défi en matière de cybersécurité pour les institutions financières. L'utilisation croissante du cloud, 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 l'échelle de ce qui doit être protégé.

Les responsables IT et les responsables des risques opérationnels se concentrent l'intégration de la sécurité dès la conception des systèmes pour gérer la croissance de l'empreinte numérique, et réduire la complexité de l'orchestration de la sécurité entre de nombreuses solutions disparates. Les professionnels de la sécurité ont besoin de fonctionnalités qu'ils peuvent faire évoluer à l'échelle de l'entreprise, sous la forme d'une solution complète, intégrée et facile à gérer. Leur objectif est d'avoir une meilleure visibilité, d'anticiper les problèmes, de prendre les mesures appropriées et de renforcer les investissements en matière de résilience de la sécurité à l'échelle de leur entreprise.

L'accélération de la transformation numérique et l'adoption de ses technologies augmentent la complexité

The bridge to possible

Sécuriser les entreprises du secteur des services financiers

La gamme Cisco® Secure offre une sécurité de pointe allant de la périphérie du cloud à l'ensemble des réseaux, des applications, des workloads, des utilisateurs et des équipements.

- Cisco Secure XDR offre des fonctionnalités de détection et de réponse étendues (XDR) qui fournissent une visibilité et des informations exploitables pour aider les équipes du SOC à identifier les menaces, à les analyser et à y remédier.
- La connectivité sécurisée Cisco s'appuie sur l'architecture de sécurité au niveau des points d'accès (SASE) en associant des fonctions de réseau et de protection dans le cloud pour fournir un accès simple et sécurisé aux applications, partout où les utilisateurs travaillent.
- Cisco Zero Trust offre une solution complète qui sécurise les accès sur l'ensemble des applications et des environnements, pour tous les utilisateurs et tous les terminaux, où qu'ils soient.
- Cisco Secure Firewall vous aide à planifier et à hiérarchiser vos tâches, à supprimer les failles et à ressortir plus fort d'un incident. Face à la décentralisation de vos équipes, données, bureaux et sites distants, vous avez besoin d'un pare-feu polyvalent.

Compter sur les bons partenaires

Si les risques liés à la cybersécurité représentent encore un défi, 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.

En savoir plus

Pour en savoir plus sur nos services et solutions pour le secteur financier, rendez-vous sur la page Cisco pour les services financiers. Pour en savoir plus sur la résilience des systèmes de sécurité, consultez notre page dédiée.

C11-3578322-00 04/23