Orange
Cyberdefense

Conformité SWIFT : Costumer security program

Sécuriser les flux bancaires : protéger vos infrastructures SWIFT

Les enjeux de la mise en conformité

La nette augmentation des attaques informatiques visant les infrastructures de gestion des flux monétaires (réseau SWIFT) a motivé le comité SWIFT a publier un référentiel de sécurité à destination de ses membres. Ce programme dénommé Customer Security Program (CSP) impose à tous les membres du réseau SWIFT des règles de sécurité strictes en matière de protection de leurs systèmes définies dans le Customer Security Controls Framework (CSCF).

Le déploiement des exigences ainsi que leur maintien peut être un enjeu de taille pour une entreprise ou un institut financier. Les mesures de sécurité se renforceront encore ses préconisations dans les années à venir.

La déclaration de conformité, basée sur une autodéclaration, est un point d'étape obligatoire qui engage la responsabilité de la Direction et doit être abordée avec prudence.

Notre accompagnement

Fort de nombreuses expériences auprès de banques, institutions financières ou de groupe du CAC40, Orange Cyberdefense propose une expertise en cybersécurité.

Notre accompagnement sur les thématiques du CSP peut se faire à plusieurs niveaux :

- **Evaluation et audit de conformité :** afin d'évaluer le niveau de conformité des mesures en place vis-à-vis des exigences du CSP, Orange Cyberdefense mandate des auditeurs qui identifieront vos lacunes et vous définiront un plan d'action concret et pragmatique. Au travers de ces éléments, vos équipes pourront sereinement valider le questionnaire et entreprendre les chantiers nécessaires à l'amélioration de la sécurité de vos infrastructures ;
- **Accompagnement à la mise en conformité :** expert dans le déploiement et la gestion des infrastructures sensibles, Orange Cyberdefense accompagne ses partenaires dans le déploiement des mesures techniques et organisationnelles imposées par le CSP ;

Quelques chiffres

- **Détournement de 101 Millions de US dollars** lors de la cyberattaque de la banque du Bangladesh
- **Plus de 10 attaques ciblées observées** depuis 2016 ciblant les infrastructures SWIFT
- **37,9 millions de messages FIN** sont envoyés **par jour** en juin 2020

La démarche

Initialisation et cadrage

Définition du périmètre soumis au CSP et du type d'architecture SWIFT

Ateliers techniques et organisationnels

Identification des contraintes, mesures mises en place, organisations et processus

Pilotage de la conformité

Identification des lacunes et définition d'un plan d'action
Ou
Accompagnement à la mise en place des exigences

Restitution

Bilan de la mission et capitalisation

Cadrage et lancement

- Identification de l'équipe projet.
- Prise de connaissance de l'existant.
- Présentation de la méthodologie d'Orange Cyberdefense.

Accompagnement / Audit

- Ateliers avec les opérationnels et les administrateurs pour faire un état de lieux.
- Identification des actions de mises en conformité et rédaction d'un plan d'action.
- Accompagnement à la mise en œuvre des mesures techniques et organisationnelles.

Bilan et capitalisation

- Accompagnement à la rédaction du questionnaire d'auto déclaration.
- Présentation des résultats de l'étude.

Vos bénéfices :

Rationaliser

- Créez une infrastructure répondant aux exigences du CSP, en cohérence avec vos pratiques et systèmes déjà en place
- Identifiez les chantiers devant être menés et établissez un planning pragmatique

Sécuriser

- Profitez d'une expertise dans le domaine de la sécurité et bancaire afin de protéger vos flux bancaires
- Via un accompagnement spécifique, déployez les mesures nécessaires et suffisantes pour faire face à vos risques

Tranquilliser

- Mettez vous en ordre de marche pour faire face aux exigences croissantes de SWIFT
- Présentez sereinement votre questionnaire autodéclaratif

Pour en savoir plus, contactez **communication.ocd@orange.com**
Nous suivre : **https://orangecyberdefense.com/fr**