RFC 2350
CERT CREDIT AGRICOLE

SOMMAIRE

1 OBJET DU DOCUMENT 3
2 INFORMATIONS PRATIQUES 4
2.1 Date de dernière mise à jour 4
2.2 Liste de diffusion 4
2.3 Mise à disposition du document 4
3 INFORMATIONS DE CONTACT 5
3.1.1 Nom de l'équipe de réponse à incident 5
3.1.2 Adresse postale 5
3.1.3 Fuseau horaire 5
3.1.4 Contact téléphonique 5
3.1.5 Adresses électronique 5
3.1.6 Clé de chiffrement associée à cert@credit-agricole.com 5
3.1.7 Composition de l'équipe 5
3.1.8 Disponibilité de service 5
4 CHARTE 7
4.1 Fiche de mission 7
4.2 Périmètre d'intervention 7
4.3 Parrainage/Affiliation 7
4.4 Autorité 7
5 POLITIQUES 8
5.1 Types d'Incidents et niveau de service 8
5.2 Coopération, Interaction et échanges d'informations 8
5.3 Communication et Authentification 9
5.3.1 Mise à disposition d'informations 9
5.3.2 Sécurité des communications 9
5.3.3 Classification des informations 9
5.3.4 Principes de communication externes sont les suivants : 9
6 SERVICES 10
7 FICHE INCIDENT TYPE 12
8 DISCLAIMER 13

1 OBJET DU DOCUMENT

Ce document contient la description du CERT Crédit Agricole conformément à la RFC 2350.
Il décrit de façon synthétique le périmètre d'intervention, l'organisation et les missions du CERT Crédit Agricole.
Les informations présentes dans ce document sont classifiées en **TLP:RED** tant que le document n'a pas été validé par les instances internes du Groupe.

2 INFORMATIONS PRATIQUES

2.1 Date de dernière mise à jour

La première version du document (version 1.0) date du 29 décembre 2014.
Ce document est la version 1.3 du 25 Août 2021.

2.2 Liste de diffusion

Le CERT-AG n'utilise pas de liste de diffusion.

2.3 Mise à disposition du document

Le document est communiqué sur demande.

3 INFORMATIONS DE CONTACT

3.1.1 Nom de l'équipe de réponse à incident

Nom : CERT Credit Agricole

Nom court : : CERT-AG

3.1.2 Adresse postale

12, Place des Etats-Unis 92127 Montrouge, France

3.1.3 Fuseau horaire

(GMT +1) / (GMT +2)

3.1.4 Contact téléphonique

Ligne fixe : **Réservé à l'interne du Groupe**

Nota : La ligne fixe du CERT est redirigée sur le portable d'astreinte y compris en HNO (24/7).

Les moyens de contacter le CERT sont disponibles sur l'Intranet du Groupe Crédit Agricole et à l'adresse : https://www.first.org/members/teams/cert-ag.

3.1.5 Adresses électronique

Pour signaler un incident au CERT, l'adresse mail à privilégier est cert@credit-agricole.com.

3.1.6 Clé de chiffrement associée à **cert@credit-agricole.com**

User ID: CERT Credit Agricole <cert@credit-agricole.com>

Key ID: D648DA81

Fingerprint: 920E47AD4664465E13690F5E7C4E2457D648DA81

cert-ag.asc : http://pgp.mit.edu/pks/lookup?op=vindex&search=0x7C4E2457D648DA81

Cette clé de chiffrement PGP doit être utilisée pour toute diffusion au CERT-AG d'informations à caractère sensible.

3.1.7 Composition de l'équipe

Le CERT est composé d'une équipe dédiée d'analystes, experts en sécurité, composée de salariés permanents de Crédit Agricole S.A.

Le CERT est sous la responsabilité de Marc-Frédéric Gomez.

3.1.8 Disponibilité de service

Tous les services du CERT fonctionnent en 24/7.

Le CERT est joignable 24 heures sur 24, 7 jours sur 7, 365 jours par an.

Un système d'astreinte primaire et secondaire est mis en œuvre pour couvrir toute la période.

En Heures Ouvrées (9H00-18H00, du lundi au vendredi), au minimum 3 personnes sont toujours disponibles.

4 CHARTE

4.1 Fiche de mission

Le CERT du Crédit Agricole est l'équipe d'investigation du groupe Crédit Agricole dédiée à la lutte contre la Cybercriminalité. Il fournit au groupe Crédit Agricole des services de surveillance afin de protéger le groupe Crédit Agricole contre les cyberattaques.

Il constitue un centre d'expertise, de veille et de traitement en cas de menace suspectée, détectée ou en cas de cyberattaque sur un SI du Groupe.

L'équipe se compose d'analystes, experts en sécurité informatique, en charge de réaliser les investigations.

Le CERT-AG a pour mission :

- D'aider toutes les sociétés du groupe Crédit Agricole en effectuant des analyses techniques approfondies sur les incidents liés à la cybercriminalité et en proposant des plans d'actions visant à réduire le risque ;
- De contribuer à la prévention de tels incidents en procédant à une surveillance du périmètre du Groupe Crédit Agricole, à des évaluations proactives de la menace et à une identification des précautions à prendre pour en minimiser les risques ;
- D'être le relai auprès des communautés sécurité (CSIRT et CERT) notamment à l'extérieur du Groupe.

4.2 Périmètre d'intervention

Le CERT Crédit Agricole est un acteur clé du dispositif de la lutte opérationnelle contre la cybercriminalité portant atteinte aux Entités du Groupe Crédit Agricole et à leurs clients.

À ce titre, ses missions s'organisent autour de la veille, de la prévention et du traitement des incidents de sécurité et de cybercriminalité impactant le SI des Entités du Groupe Crédit Agricole et de leurs filiales relevant des métiers de la banque de proximité, de l'épargne, de l'assurance, de l'immobilier, des Grandes Clientèles et des services financiers spécialisés (cf. http://www.credit-agricole.com).

4.3 Parrainage/Affiliation

Les missions du CERT sont décidés et validés par une instance représentative du Groupe Crédit Agricole.

4.4 Autorité

Le CERT Crédit Agricole agit sous l'autorité du CISO groupe.

Il travaille en étroite collaboration avec les CISO du Groupe et leurs équipes ainsi qu'avec les SOC[1] du Groupe.

[1] Security Operation Center

5 POLITIQUES

5.1 Types d'Incidents et niveau de service

Dans le cadre du dispositif de la lutte opérationnelle contre la cybercriminalité, le CERT assure la veille, la prévention et le traitement des incidents de sécurité (incidents transverses ou à la demande d'une Entité) impactant les systèmes d'informations d'une ou plusieurs Entités du Groupe Crédit Agricole.

Le CERT Crédit Agricole intervient sur tout incident du domaine de la sécurité ou de la cybercriminalité impactant de façon potentielle ou avérée les Entités du Groupe Crédit Agricole.

Le CERT peut être mandaté par des Entités pour des expertises spécifiques nécessitant d'accéder à des équipements sensibles (tels que des automates de retrait ou des serveurs), à des équipements de collaborateurs (tels que des PC ou des smartphones) ou encore à des journaux d'équipements réseau ou de sécurité. Dans ces cas d'expertises techniques nécessitant l'accès à des données à caractère personnel ou à des données sensibles, un mandat spécifique sera rédigé pour préciser le cadre de la mission confiée au CERT.

Le CERT s'engage à donner une suite à tout signalement envoyé concernant son périmètre, soit par une réponse individuelle, soit par un message envoyé à toutes les Entités concernées dans le cas d'une réponse d'intérêt général.

Toute alerte (i.e. signalement d'un incident présentant un caractère d'urgence compte-tenu des impacts potentiels ou avérés ou de la criticité du système impacté) doit être matérialisée par un appel téléphonique. Le CERT s'engage à prendre en compte l'alerte dans les 15 minutes qui suivent sa réception.

Le CERT s'engage à débuter le traitement proprement dit de l'alerte au plus tard dans l'heure qui suit sa réception.

Dans la mesure du possible, les incidents les plus critiques sont pris en charge dans les 15 minutes qui suivent leur signalement.

5.2 Coopération, Interaction et échanges d'informations

Le CERT-AG considère essentiel de créer une coopération avec des communautés de sécurité, CERT et CSIRT. Le CERT échange essentiellement retours d'expériences et informations pertinentes de façon à renforcer la capacité à détecter et à traiter les incidents de sécurité.

Les informations échangées par le CERT-AG avec l'ensemble de la communauté de sécurité, CERT/CSIRT se limitent aux informations techniques dans son domaine de responsabilité et strictement nécessaires. Aucune donnée spécifique au Groupe ou donnée à caractère personnel n'est échangée sans l'accord explicite des personnes habilitées et concernées.

5.3 Communication et Authentification

5.3.1 Mise à disposition d'informations

Les communications réalisées par le CERT sont de plusieurs types :

- Alertes ciblées à destination des Entités
- Articles sur l'activité (disponible sur le blog du CERT)
- Revue de presse (disponible sur le blog du CERT et envoyé par mail à une liste de CISO/RSI et personnes intéressées)
- Statistiques quotidiennes sur le phishing
- Statistiques annuelles, mensuelles et hebdomadaires
- Guide sécurité
- Lettre mensuelle
- Interventions pour informer /sensibiliser sur la menace, dispensées à la demande des Entités (ou de Crédit Agricole SA.

5.3.2 Sécurité des communications

Les communications téléphoniques du CERT sont non chiffrées.

Les mails sont par défaut envoyés non chiffrés.

Le CERT dispose d'une clé de chiffrement disponible sur l'intranet mais également publiée au MIT (http://pgp.mit.edu/) pour que les expéditeurs de mails à destination du CERT puissent chiffrer les mails ou les pièces jointes contenant des informations sensibles.

5.3.3 Classification des informations

Le CERT respecte les règles Groupe en matière de confidentialité concernant l'échange et le stockage de données sensibles ou à caractère personnel.

Lors de ses échanges avec d'autres communautés sécurité, le CERT respecte les règles de confidentialité dites « TLP » pour Traffic Light Protocol.

5.3.4 Principes de communication externes sont les suivants :

5.3.4.1 Communication vers le grand public

Le CERT ne communique pas vers le grand public.

Une exception à cette règle, la publication d'alertes de sécurité sur le Guide Sécurité Groupe ouvert sur Internet.

5.3.4.2 - Communication vers les autorités et organismes officiels

Le CERT communique vers les Autorités et Organismes officiels. Ces communications sont soumises aux règles TLP et aux règles spécifiques de l'Autorité en question.

En cas de doute, le CERT se rapproche des juristes de Crédit Agricole SA.

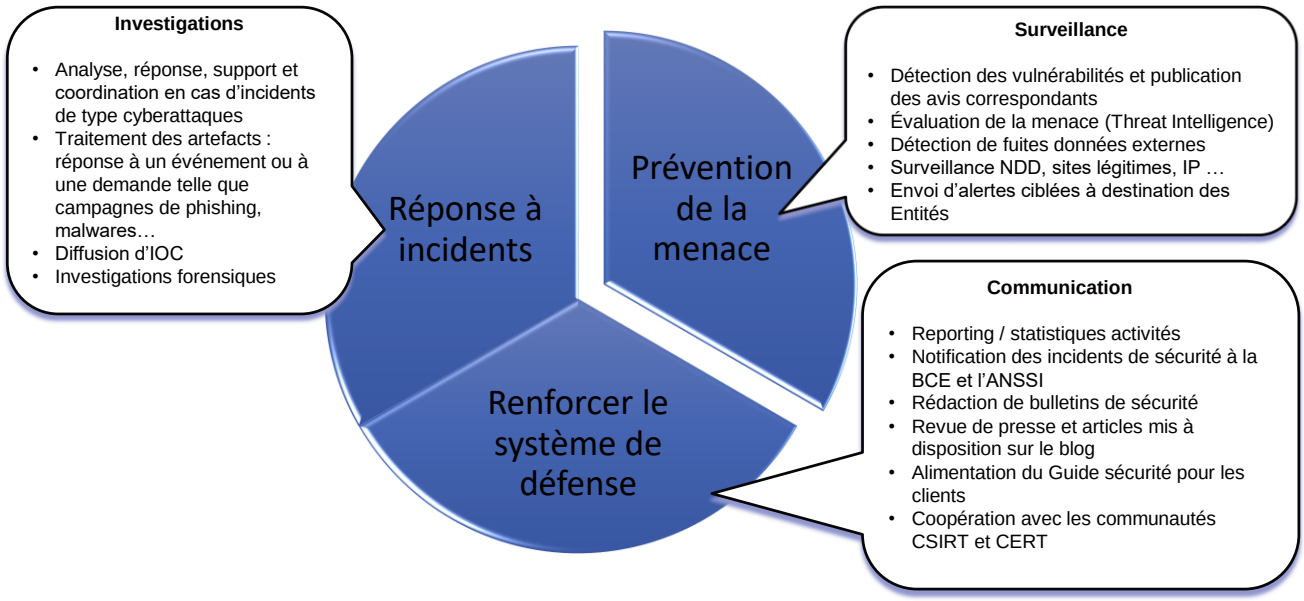
5.3.4.3 - Communication vers les partenaires

L'écosystème externe du CERT comprend les acteurs suivants : communautés des CERT et CSIRT, communautés fermées (accès par cooptation) de sécurité et de lutte contre la cybercriminalité françaises et étrangères, conférences.

6 SERVICES

Le CERT propose des services d'expertise technique sur les domaines relevant de la cybercriminalité :

- Investigations dans le cadre de la réponse à incidents : analyse de phishing, analyse de malwares, fuite de données (Cartes bancaires, données personnelles clients ...), fraudes bancaires, analyse forensique ;
- Surveillance pour prévenir la menace : Surveillance et anticipation des attaques de phishing et de malwares, Surveillance des noms de domaine du Groupe Crédit Agricole, surveillance de la réputation des IP du Groupe, surveillance des applications mobiles, veille sur les vulnérabilités et les attaques génériques ou ciblées Crédit Agricole ;
- Communication visant à renforcer le système de défense : Préconisations techniques, bonnes pratiques ; Conseil pour les notifications obligatoires d'incidents de sécurité du Groupe Crédit Agricole aux autorités et organismes officiels, Conseil pour la communication externe (clients du Groupe Crédit Agricole) sur les menaces.



Présentation synthétiques des services du CERT

Les actions prioritaires du CERT sont résumées ci-après.

- Alerter les Entités du Groupe CA sur les attaques potentielles ou avérées, diffuser des informations sur les précautions à prendre pour minimiser les risques d'incident ou à défaut leurs conséquences.
- Centraliser et répondre aux demandes d'assistance des Entités du Groupe Crédit Agricole suite à des cyberattaques relevant du périmètre du CERT (prise en compte des demandes, diagnostic technique des alertes reçues, analyse des symptômes et corrélation des incidents).
- Fournir l'analyse technique et rédiger les propositions d'amélioration et de mesures correctives en réaction aux attaques.
- Assurer la coordination entre les différentes Entités concernées, le suivi de situation et du plan d'actions associé (gestion d'incidents de sécurité, gestion de crise).
- Établir et maintenir une base des vulnérabilités.

Le CERT s'engage à communiquer aux Entités pour les informer de toute menace potentielle ou avérée les ciblant.

Les messages émis par le CERT sont classés en niveaux en fonction de la criticité de l'incident identifié.

Une alerte descendante peut être émise par le CERT vers les Entités du Groupe pour :

- Demander une action locale,
- Demander une investigation locale et la remontée au CERT des informations recueillies,
- Transmettre une information sans action associée.

7 FICHE INCIDENT TYPE

Il n‘existe pas de format de fiche incident imposé.

Le format de signalement privilégié et le mail.

8 DISCLAIMER

Les services du CERT sont rendus de la manière la plus efficace possible mais, malgré toutes les précautions prises, il est possible que certaines actions ne soient pas pleinement efficaces à ce jour.