CSIRT Bourgogne Franche-Comté

RFC 2350

SOMMAIRE

1 A propos du document

Ce document contient une description de l'ARNia Cybersécurité – CSIRT-BFC tel que recommandé par la RFC2350[1]. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT-BFC.

1.1 Date de la dernière mise à jour

Ceci est la version 2.0 de ce document, éditée le 17 novembre 2022

1.2 Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants :
https://www.csirt-bfc.fr

1.3 Où trouver ce document

Ce document peut être trouvé sur le site du CSIRT-BFC : https://www.csirt-bfc.fr

1.4 Authenticité du document

Ce document a été signé à l'aide de la clé PGP du CSIRT-BFC.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet du CSIRT-BFC à l'adresse suivante :
https://www.csirt-bfc.fr

1.5 Identification du document

Titre : RFC 2350 du CSIRT-BFC
Version : 2.0
Date de mise à jour : 17 novembre 2022
Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

[1] http://www.ietf.org/rfc/rfc2350.txt

2 Informations de contact

2.1 Nom de l'équipe

Nom court : CSIRT-BFC
Nom complet : CSIRT Bourgogne-Franche-Comté

2.2 Adresse

CSIRT Bourgogne-Franche-Comté
ARNIA, Agence Régionale du Numérique et de l'Intelligence Artificielle
3 bis rue du Suzon 21000 DIJON

2.3 Zone horaire

CET/CEST : Paris (GMT+01:00, et GMT+02:00 heure d'été)

2.4 Numéro de téléphone

0 970 609 909

2.5 Numéro de Fax

Aucun à ce jour.

2.6 Autres moyens de communication

Aucun à ce jour.

2.7 Adresse E-Mail

cyber_at_arnia-bfc.fr

2.8 Clé publique et informations liées au chiffrement

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec le CSIRT-BFC.
Identifiant utilisateur : ARNia Cybersécurité – CSIRT-BFC
Identifiant de la clé : cyber_at_arnia-bfc.fr
Empreinte : 169A B32B
La clé PGP publique est disponible à cette adresse : https://www.csirt-bfc.fr ainsi que sur les principaux serveurs de clés PGP :

- https://pgp.circl.lu
- https://pgp.mit.edu
- https://keys.openpgp.org

- https://keyserver.ubuntu.com
- https://keyserver.pgp.com

2.9 Membres de l'équipe

L'équipe est constituée de plusieurs membres :

- Un responsable;
- Plusieurs analystes.

2.10Autres informations

Aucune à ce jour.

2.11Contact

Le CSIRT-BFC est disponible durant les heures ouvrées, soit de 09h00 à 12h30 et de 13h30 à 17h00, du lundi au vendredi (hors jours fériés).

Pour joindre le CSIRT-BFC, le moyen de communication privilégié est le numéro de téléphone 0 970 609 909 et, en seconde intention, par courriel à l'adresse cyber_at_arnia-bfc.fr

Nous encourageons l'utilisation de chiffrement avec les informations présentées dans le paragraphe 2.8 Clé publique et informations liées au chiffrement pour assurer l'intégrité et la confidentialité des échanges.

3 Charte

3.1 Ordre de mission

Le CSIRT-BFC est l'équipe de réponse aux incidents de sécurité informatique de la région Bourgogne-Franche-Comté. Son objectif est d'apporter une assistance aux organisations de son territoire (décrites dans le paragraphe 3.2 Bénéficiaires) pour répondre aux incidents cyber auxquels elles font face.

3.2 Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT-BFC sont les organisations localisées sur le territoire de la région Bourgogne-Franche-Comté, comprenant notamment :

- Les PME ;
- Les ETI ;
- Les collectivités territoriales et les établissements publiques associés ;
- Les associations.

3.3 Affiliation

Ce CSIRT-BFC est affilié à la l'Agence Régionale du Numérique et de l'intelligence artificielle de la Région Bourgogne-Franche-Comté.

3.4 Autorité

Le CSIRT-BFC réalise ses activités sous l'autorité de l'Agence Régionale du Numérique et de l'Intelligence Artificielle (ARNia), dont la région Bourgogne-Franche-Comté est membre fondateur.

4 Politiques

4.1 Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT-BFC couvre tous les incidents de sécurité informatique touchant les organisations de son territoire décrites dans le paragraphe 3.2 Bénéficiaires.
Les missions principales du CSIRT-BFC sont :

- Offrir une réponse de premier niveau pour les incidents cyber survenant chez ses bénéficiaires ;
- Rediriger ses bénéficiaires vers des prestataires régionaux pour la remédiation de l'incident ;
- Agir comme un relai entre le CERT-FR, les prestataires régionaux, les services de Police et de Gendarmerie et les bénéficiaires ;
- Consolider les statistiques d'incidentologie à l'échelle régionale.

4.2 Coopération, interaction et partage d'information

Les informations relatives à un incident telles que le nom de la structure et les détails techniques ne sont pas publiées sans l'accord de la partie nommée.
Le CSIRT-BFC peut être amené à communiquer des informations aux autres CSIRT régionaux ou au CERT-FR lorsqu'une structure sollicite leur appui. De la même manière, des informations pourront être partagées à un CSIRT sectoriel (santé, maritime…) à des fins de capitalisation des incidents propres au secteur concerné.
La diffusion d'information sera traitée en accord avec le protocole TLP défini par FIRST (https://www.first.org/tlp).

4.3 Communication et authentification

Le CSIRT-BFC conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.
Les informations non confidentielles ou peu sensibles peuvent être transmises via des courriels non chiffrés.

5 Services

5.1 Réponse aux incidents

L'activité principale du CSIRT-BFC est de venir en aide à ses bénéficiaires en proposant un service de réponse de premier niveau aux incidents cyber et de les aider à affiner leur choix de prestataire pour les accompagner dans la suite de la résolution des incidents.
En particulier, il propose les services détaillés dans les paragraphes suivants.

5.1.1 Triage

- Récupération du signalement et prise de contact avec le déclarant ;
- Collecte d'informations sur l'incident et confirmation ou évaluation de la nature de l'incident ;
- Détermination de la sévérité de l'incident (son impact) et de son périmètre (nombre de machines affectés) ;
- Catégorisation de l'incident.

5.1.2 Coordination

- Identification du meilleur partenaire au sein du dispositif national de réponse aux incidents pour accompagner le demandeur ;
- Accompagnement dans la diffusion, le cas échéant, de signalements vers les autorités compétentes de l'Etat selon la nature de l'incident. Notamment, mais de manière non exhaustive :
    - A l'ANSSI en cas d'incident majeur de cybersécurité pouvant impacter d'autres secteurs ;
    - A la Commission Nationale de l'Informatique et des Libertés (CNIL) en cas de violation de données à caractère personnel.

5.1.3 Résolution

- Proposition d'actions réflexes, notamment des mesures d'urgence pour limiter l'impact de l'incident ou des mesures destinées à faciliter les investigations et le traitement de l'incident ;
- Partage d'une liste restreinte de prestataires de proximité capables d'assurer la résolution et la remédiation de l'incident ;
- Suivi des phases de résolution et de remédiation.

5.2 Activités proactives

Le CSIRT-BFC pourra aussi proposer des services proactifs à ses bénéficiaires, notamment :

- Des services de veille ;
- Des analyses de menaces ;
- Un bulletin de veille à destination d'abonnés.

6 Formulaires de notification d'incident

Un formulaire de notification est disponible en ligne à cette adresse :

https://www.csirt-bfc.fr/contact.php

En cas de déclaration par courriel, pour faciliter la prise en compte des signalements, les éléments suivants sont si possibles à fournir :

- Informations sur l'organisation touchée (nom, contact de la direction et des équipes techniques, taille…) ;
- Informations de contact du demandeur comprenant notamment : nom, fonction et numéro de téléphone ;
- Chronologie de l'incident : date et heure du début de l'incident et de sa détection ;
- Description de l'incident comprenant notamment l'impact sur l'organisation et le nombre et type de machines touchées ;
- Actions effectuées depuis la détection de l'incident ;
- Toute autre résultat d'investigations déjà menées ;
- Architecture du système d'informations ;
- Outils et politiques de défense contre les incidents en place ;
- Si le demandeur est déjà en contact avec un prestataire de réponse aux incidents de sécurité informatique ;
- Services attendus de la part d'une équipe de réponse aux incidents.

7 Décharge de responsabilité

Bien que toutes les précautions soient prises dans la préparation des informations, notifications et alertes, le CSIRT-BFC n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues.