CSIRT NORMANDIE CYBER

RFC2350

AVRIL 2022

Contrôle du document				
	Prénom Nom	Fonction	Date	
Rédaction	Stéphane BRESSON	Resp. Départ.	20/4/22	
Approbation	Jérome LE TENSORER	DGA	2/5/22	

Historique des versions			
Version	Date	Auteur	Nature
V 1.1	20 Avril 2022	SB	création
V1.2	11 mai 2022	SB	Mise à jour

TLP:WHITE

CSIRT Normandie Cyber– RFC2350

Table des matières

Table des matières **1**

1. À propos du document **2**
1.1 Date de dernière mise à jour *2*
1.2 Liste de distribution pour les modifications *2*
1.3 Où trouver ce document *2*
1.4 Authenticité du document *2*
1.5 Identification du document *2*

2. Informations de contact **2**
2.1 Nom de l'équipe *2*
2.2 Adresse *2*
2.3 Zone horaire *2*
2.4 Numéro de téléphone *2*
2.5 Numéro de Fax *3*
2.6 Autres moyens de communication *3*
2.7 Adresse E-Mail *3*
2.8 Clé publique et informations liées au chiffrement *3*
2.9 Membres de l'équipe *3*
2.10 Autres informations *3*
2.11 Contact *3*

3. Charte **4**
3.1 Ordre de mission *4*
3.2 Bénéficiaires *4*
3.3 Affiliation *4*
3.4 Autorité *4*

4. Politiques **4**
4.1 Types d'incidents et niveau d'intervention *4*
4.2 Coopération, interaction et partage d'information *5*
4.3 Communication et authentification *5*

5. Services **6**
5.1 Réponse aux incidents *6*
5.1.1 Triage 6
5.1.2 Coordination 6
5.1.3 Résolution 6
5.2 Activités proactives *6*

6. Formulaires de notification d'incident **7**

7. Décharge de responsabilité **7**

TLP:WHITE

CSIRT Normandie Cyber– RFC2350

1. À propos du document

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

1.1 Date de dernière mise à jour

Ceci est la version 1.1 de ce document, éditée le 10/4/2022

1.2 Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants :

- InterCERT-FR / réseau de Français CSIRT - www.cert.ssi.gouv.fr/csirt/intercert-fr

Veuillez envoyer des questions sur les mises à jour de l'adresse e-mail de l'équipe CSIRT NORMANDIE CYBER contact@normandie-cyber.fr

1.3 Où trouver ce document

Ce document peut être trouvé sur le site du CSIRT NORMANDIE CYBER : www.normandie-cyber.fr

1.4 Authenticité du document

-

1.5 Identification du document

Titre : RFC 2350 du CSIRT NORMANDIE CYBER
Version : 0.1
Date de mise à jour : 1.4/22
Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

2. Informations de contact

2.1 Nom de l'équipe

Nom court : NORMANDIE CYBER
Nom complet : CSIRT NORMANDIE CYBER

2.2 Adresse

Adnormandie 2 Esplanade Anton Philips 14460 Colombelles

2.3 Zone horaire

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

2.4 Numéro de téléphone

0808 800 001

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

2.5 Numéro de Fax

-

2.6 Autres moyens de communication

-

2.7 Adresse E-Mail

contact@normandie-cyber.fr

2.8 Clé publique et informations liées au chiffrement

A17B2B7FBEE89EE8EB14940F4739FCA15494D873

2.9 Membres de l'équipe

L'équipe est constituée de 2 personnes :

- Un responsable du CSIRT ;
- un analyste.

Aucune information nominative relative aux membres du CSIRT n'est diffusée dans ce document.

2.10 Autres informations

Aucune à ce jour.

2.11 Contact

Le CSIRT NORMANDIE CYBER est disponible durant les heures ouvrées, soit de 8 heures à 17 heures du lundi au jeudi et de heures à 16h le vendredi (hors jours fériés).

Pour joindre le CSIRT NORMANDIE CYBER, le moyen de communication privilégié est par courriel à l'adresse contact@normandie-cyber.fr. En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre courriel.

Le CSIRT NORMANDIE CYBER est aussi joignable par téléphone au 0808 800 001

En dehors de ces heures les adhérents peuvent signaler leur incident auprès de l'Agence Nationale de la sécurité des Systèmes d'Information (ANSSI) dont les coordonnées figurent à l'adresse suivante : http://www.cert.ssi.gouv.fr/contact/,

ou bien auprès du site : www.cybermalveillance.gouv.fr/diagnostic

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 NORMANDIE CYBER est l'équipe de réponse aux incidents de sécurité informatique de la région Normandie. 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.

Les missions du CSIRT NORMANDIE CYBER sont :

- Accompagner les bénéficiaires du dispositif (§ 3.2) victimes d'un incident informatique et les orienter vers des prestataires en sécurité informatique, référencés de la région
- Assurer une veille à partir de l'écosystème cybersécurité régional et national sur les menaces et les vulnérabilités ;
- Alerter les bénéficiaires de ces menaces et vulnérabilités ;
- Contribuer à la sensibilisation des entreprises de la région de manière permanente en relayant les informations disponibles auprès des organismes d'état et d'entreprises spécialisées en cybersécurité.

3.2 Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT NORMANDIE CYBER sont les organisations localisées sur le territoire de la région Normandie, appartenant aux catégories suivantes :

- Les PME ;
- Les ETI ;
- Les collectivités territoriales et les établissements publiques associés de taille moyenne (de plus de 5 000 habitants ;

3.3 Affiliation

Ce CSIRT est affilié à la Région Normandie

3.4 Autorité

Le CSIRT NORMANDIE CYBER réalise ses activités sous l'autorité de l'Agence de Développement pour la Normandie (ADNormandie), elle-même sous l'autorité de la Région Normandie.

4. Politiques

4.1 Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT NORMANDIE CYBER 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 NORMANDIE CYBER 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 en tant que relai pour les bénéficiaires auprès du CERT-FR, des prestataires régionaux, des services de Police et de Gendarmerie ;
- Consolider les statistiques d'incidentologie à l'échelle régionale.

Le CSIRT NORMANDIE CYBER est autorisé à coordonner et assurer un premier diagnostic de tout incident de sécurité informatique qui cible ou pourrait cibler un de ses bénéficiaires. En fonction de la nature de l'incident, le CSIRT NORMANDIE CYBER propose une liste de prestataire en Cybersécurité, susceptible d'aider l'entreprise dans la résolution de l'incident. Un suivi de la résolution de l'incident est assuré afin de statistiques et de capitalisation, et pour améliorer les capacités de diagnostic.

Le niveau de support offert par le CSIRT NORMANDIE CYBER peut varier en fonction du type d'incident, de sa criticité, et des ressources disponibles pour le prendre en charge. Dans le cas où l'incident concerne une structure non bénéficiaire, celle-ci pourra être redirigée vers d'autres centres de réponse à incident : ANSSI, Cybermalveillance, CSIRT sectoriel...

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 NORMANDIE CYBER 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.

Toutes les informations sont transmises en fonction de leur classification et du principe du besoin de savoir. Seuls les extraits spécifiquement pertinents et anonymisés sont transmis. Le CSIRT NORMANDIE CYBER traite l'information dans des environnements physiques et techniques sécurisés conformément aux réglementations existantes en matière de protection de l'information.

4.3 Communication et authentification

Le CSIRT NORMANDIE CYBER 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 sensibles peuvent être transmises via des courriels non chiffrés.

La diffusion d'information sera traitée en accord avec le protocole TLP défini par FIRST (https://www.first.org/tlp).

5. Services

5.1 Réponse aux incidents

L'activité principale du CSIRT NORMANDIE CYBER 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 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 ;
- Compte rendu d'intervention concernant le traitement de l'incident et capitalisation de la connaissance

5.1.3 Coordination

- Identification du meilleur partenaire au sein du dispositif national[2] 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.

5.2 Activités proactives

Le CSIRT NORMANDIE CYBER 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.

[2] Redirection éventuelle vers ACYMA, le CERT-FR ou autre CSIRT (e.g. sectoriel)

6. Formulaires de notification d'incident

Un formulaire permettant de notifier le CSIRT NORMANDIE CYBER d'un incident est disponible sur le site www. Normandie-cyber.fr ainsi que sur le site de l'ADNormandie

Pour faciliter la prise en compte des signalements, les éléments suivants sont à fournir :

- Informations sur l'organisation touchée (nom, SIRET, contact de la direction et des équipes techniques, taille, localisation…) ;
- Informations de contact du demandeur comprenant notamment : nom, fonction et numéro de téléphone ;
- Qualification de l'incident : Chronologie (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 et tout autre résultat d'investigations déjà menées ;
- Si le demandeur est déjà en contact avec un prestataire de réponse aux incidents de sécurité informatique, ses coordonnées ;

7. Décharge de responsabilité

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

Si vous constatez une erreur dans ce document merci de nous le signaler par mail. Nous tâcherons de rectifier les informations au plus vite