

CSIRT PAYS DE LA LOIRE CYBER ASSISTANCE

RFC2350

23/10/2023

SOMMAIRE

A PROPOS DU DOCUMENT	4
Date de dernière mise à jour	4
Liste de distribution pour les modifications	4
Où trouver ce document	4
Authenticité du document	4
Identification du document	4
INFORMATIONS DE CONTACT	5
Nom de l'équipe	5
Adresse	5
Zone horaire	5
Numéro de téléphone	5
Numéro de fax	5
Autres moyens de communication	5
Adresse E-Mail	5
Clé publique et informations liées au chiffrement	6
Membres de l'équipe	6
Autres informations	6
Contact	6
CHARTRE	7
Ordre de mission	7
Bénéficiaires	7
Affiliation	7
Autorité	7
POLITIQUES	8
Types d'incidents et niveau d'intervention	8
Coopération, interaction et partage d'information	8
Communication et authentification	8

SERVICES.....	9
Réponse aux incidents.....	9
Triage.....	9
Coordination.....	9
Résolution.....	9
Activités proactives	10
FORMULAIRES DE NOTIFICATION D’INCIDENT.....	11
DECHARGE DE RESPONSABILITE.....	11

A PROPOS DU DOCUMENT

Ce document contient une description du CSIRT Pays de la Loire Cyber Assistance de la Région des Pays de la Loire, tel que recommandé par la RFC2350¹. Il présente des informations sur l'équipe, les services proposés et les moyens de contacter le CSIRT Pays de la Loire Cyber Assistance.

Date de dernière mise à jour

Ceci est la version 1.0 de ce document, éditée le 23/10/2023.

Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants : [CSIRT Pays de la Loire Cyber Assistance – RFC2350.pdf](#)

Où trouver ce document

Ce document peut être trouvé sur le site de la Région Pays de la Loire : [CSIRT Pays de la Loire Cyber Assistance – RFC2350.pdf](#)

Authenticité du document

Ce document a été signé à l'aide de la clé PGP du CSIRT Pays de la Loire Cyber Assistance.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet de Région Pays de la Loire à l'adresse suivante : [CSIRT Pays de la Loire Cyber Assistance – RFC2350.pdf](#)

Identification du document

Titre : RFC 2350 du CSIRT Pays de la Loire Cyber Assistance

Version : 1.0

Date de mise à jour : 23/10/2023

Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

¹ <http://www.ietf.org/rfc/rfc2350.txt>

INFORMATIONS DE CONTACT

Nom de l'équipe

Nom court : Pays de la Loire Cyber Assistance

Nom complet : CSIRT Pays de la Loire Cyber Assistance

Adresse

Conseil régional des Pays de la Loire
CSIRT Pays de la Loire Cyber Assistance
1, rue de la Loire
44966 Nantes Cedex 9

Zone horaire

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

Numéro de téléphone

0 800 100 200

Numéro de fax

Non applicable

Autres moyens de communication

Non applicable

Adresse E-Mail

cyberassistance@paysdelaloire.fr

Clé publique et informations liées au chiffrement

PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec le CSIRT Cyber Assistance

Identifiant utilisateur : cyberassistance@paysdelaloire.fr

Identifiant de la clé : 0x2C3D542D

Empreinte : ED9C 60A1 9598 EA3D 3828 083F B73E 249B 2C3D 542D

La clé PGP publique est disponible à cette adresse : [CSIRT Pays de la Loire Cyber Assistance – RFC2350.pdf](#) ainsi que sur les principaux serveurs de clés PGP (MIT, CIRCL) tels que : [Clé PGP](#)

Membres de l'équipe

L'équipe est constituée de :

- Un responsable du CSIRT
- Un analyste
- Un opérateur de centre d'appel de téléphonie, expert en cybersécurité

Le responsable du CSIRT Pays de la Loire Cyber Assistance est Alex CHAUVELIN.

Autres informations

Aucune à ce jour.

Contact

Le CSIRT Pays de la Loire Cyber Assistance est disponible 24H/24 et 7/7 (hors jours fériés) par téléphone.

Pour joindre le CSIRT Pays de la Loire Cyber Assistance, le moyen de communication privilégié est par courriel à l'adresse cyberassistance@paysdelaloire.fr.

Nous encourageons l'utilisation de chiffrement avec les informations présentées dans le paragraphe « [Clé publique et informations liées au chiffrement pour assurer l'intégrité de la confidentialité des échanges](#) ».

En cas d'urgence, veuillez spécifier la balise [URGENT] dans le champ objet de votre courriel.

Le CSIRT Pays de la Loire Cyber Assistance est aussi joignable par téléphone au 0 800 100 200.

CHARTRE

Ordre de mission

Le CSIRT Pays de la Loire Cyber Assistance est l'équipe de réponse aux incidents de sécurité informatique de la région Pays de la Loire. Son objectif est d'apporter une assistance aux organisations de son territoire (décrites dans le paragraphe « [Bénéficiaires](#) ») pour répondre aux incidents de cybersécurité auxquels elles font face.

Bénéficiaires

Les entités pouvant bénéficier de l'accompagnement du CSIRT Pays de la Loire Cyber Assistance sont les organisations localisées sur le territoire de la région Pays de la Loire, comprenant notamment :

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

Affiliation

Ce CSIRT est affilié à la région Pays de la Loire.

Autorité

Le CSIRT Pays de la Loire Cyber Assistance réalise ses activités sous l'autorité du service de la direction de la transformation numérique, lui-même sous l'autorité de la région Pays de la Loire.

POLITIQUES

Types d'incidents et niveau d'intervention

Le périmètre d'action du CSIRT Pays de la Loire Cyber Assistance couvre tous les incidents de sécurité informatique touchant les organisations de son territoire décrites dans le paragraphe « [Bénéficiaires](#) ».

Les missions principales du CSIRT Pays de la Loire Cyber Assistance 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.

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 Pays de la Loire Cyber Assistance 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>).

Communication et authentification

Le CSIRT Pays de la Loire Cyber Assistance 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.

SERVICES

Réponse aux incidents

L'activité principale du CSIRT Pays de la Loire Cyber Assistance 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.

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.

Coordination

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

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.

Activités proactives

Le CSIRT Pays de la Loire Cyber Assistance 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 ;
- De la formation ;
- Du conseil ;
- De l'assistance.

FORMULAIRES DE NOTIFICATION D'INCIDENT

Aucun formulaire permettant de notifier le CSIRT Pays de la Loire Cyber Assistance d'incidents n'a été développé à ce jour.

En revanche, 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.

DECHARGE DE RESPONSABILITE

Bien que toutes les précautions soient prises dans l'orientation des usagers du CSIRT, Pays de la Loire Cyber assistance ne peut être tenu responsable des erreurs ou omissions, ou des dommages pouvant résulter de l'utilisation des informations fournies dans le cadre de l'appui au traitement d'un incident et des actions entreprises sur les systèmes.