Breizh Cyber

LE CENTRE DE RÉPONSE AUX INCIDENTS CYBER

RFC 2350

Table des matières

Historique des versions

Version	Date	Rédaction	Validation	Description
1.0	18/10/2023	Valentin Chuzel	Guillaume Chéreau	Création
1.1	05/12/2023	Valentin Chuzel	Guillaume Chéreau	Modifications des services

1. À propos du document

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

1.1 Liste de distribution pour les modifications

Toutes les modifications apportées à ce document seront partagées via les canaux suivants :
https://breizhcyber.bzh

1.2 Où trouver ce document

Ce document peut être trouvé sur le site de Breizh Cyber :
https://breizhcyber.bzh/qui-sommes-nous/

1.3 Authenticité du document

Ce document a été signé à l'aide de la clé PGP de Breizh Cyber.

La clé PGP publique, son identifiant et son empreinte sont disponibles sur le site internet de Breizh Cyber à l'adresse suivante :
https://breizhcyber.bzh/app/uploads/2023/11/Breizh_Cyber_PGP_Key.txt

1.4 Identification du document

Titre : RFC 2350 de Breizh Cyber
Version : 1.1
Date de mise à jour : 05/12/2023
Durée de validité : ce document est valide tant qu'il n'existe pas de version ultérieure.

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

2. Informations de contact

2.1 Nom de l'équipe
Nom complet : Breizh Cyber – Le centre de réponse aux incidents cyber
Nom court : Breizh Cyber

2.2 Adresse
Breizh Cyber
5 rue de la Chataigneraie
35511 Cesson-Sévigné

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

2.4 Numéro de téléphone
0800 200 008

2.5 Numéro de Fax
Non applicable

2.6 Autres moyens de communication
Non applicable

2.7 Adresse E-Mail
contact@breizhcyber.bzh

2.8 Clé publique et informations liées au chiffrement
PGP est utilisé pour garantir la confidentialité et l'intégrité des échanges avec Breizh Cyber.

Identifiant utilisateur : contact@breizhcyber.bzh
Identifiant de la clé : C58B 7042 4D02 117C
Empreinte : 007F DDE4 A21C 9F1E 2228 8DC1 C58B 7042 4D02 117C

La clé PGP publique est disponible à cette adresse :
https://breizhcyber.bzh/app/uploads/2023/11/Breizh_Cyber_PGP_Key.txt

2.9 Membres de l'équipe
L'équipe de Breizh Cyber est composée d'analystes ou de spécialistes de la cybersécurité. Pour des raisons de confidentialité, les noms des membres de l'équipe ne sont pas rendus publics. Veuillez contacter directement Breizh Cyber pour de plus amples informations.

2.10 Autres informations
Aucune à ce jour.

2.11 Contact
Breizh Cyber est joignable durant les heures ouvrées, soit de 9 heures à 17 heures 30 du lundi au jeudi et de 9 heures à 17 heures le vendredi (hors jours fériés).

Pour joindre Breizh Cyber, les moyens de communication privilégiés sont :

- le téléphone au 0 800 200 008
- le courriel à l'adresse contact@breizhcyber.bzh
- le site web via le menu « Contact »

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

Breizh Cyber est l'équipe de réponse aux incidents de sécurité informatique de la région Bretagne. 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 de Breizh Cyber sont les organisations localisées sur le territoire de la région Bretagne, comprenant notamment :

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

Les secteurs suivants, couverts par des CERT sectoriels, sont exclus du champ de compétences de Breizh Cyber :

- La santé ;
- Le maritime ;
- L'aviation civile ;
- L'enseignement supérieur et la recherche ;
- La défense et l'armement.

3.3 Affiliation

Breizh Cyber est affilié à la région Bretagne.

3.4 Autorité

Breizh Cyber réalise ses activités sous l'autorité du président de la région Bretagne.

4. Politiques

4.1 Types d'incidents et niveau d'intervention

Le périmètre d'action de Breizh Cyber couvre tous les incidents de sécurité informatique touchant les organisations de son territoire décrites dans le paragraphe 3.2 *Bénéficiaires*.

Les missions principales de Breizh 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 ;
- Assurer des conseils en gestion de crise à un niveau stratégique en complément de la réponse à incident ;
- Mener de la recherche de données en source ouverte dans le cadre d'une réponse à incident ;
- Mener des campagnes de détection de vulnérabilité ;
- 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, ni partagées sans l'accord de la partie nommée.

Breizh 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.

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

Breizh Cyber conseille fortement l'utilisation de canaux de communication sécurisés et du chiffrement PGP, en particulier pour communiquer des informations confidentielles ou sensibles.

Breizh Cyber à fait le choix de l'outil BlueFiles pour transmettre les données sensibles et PGP pour signer/chiffrer les courriels sensibles.

Les informations non confidentielles ou sensibles (peuvent être transmises via des courriels non chiffrés.

5. Services

5.1 Réponse aux incidents

L'activité principale de Breizh 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 affectées) ;
- Catégorisation de l'incident.

5.1.2 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.

5.1.3 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 ;
- Conseils en gestion de crise à un niveau stratégique en complément de la réponse à incident ;
- Recherche de données en source ouverte en appui d'une réponse à 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 Scan de vulnérabilité sur surface d'attaque externe

Breizh Cyber s'emploie également à réduire le nombre d'équipements susceptibles d'être exploités par des attaquants. Ainsi, ces scans de vulnérabilité permettent d'évaluer la surface d'attaque des services exposés sur Internet et de contrôler que des vulnérabilités connues et activement exploitées par les attaquants n'affectent pas ces services.

Afin de respecter le périmètre régional, seuls les noms de domaine ayant pour TLD « .bzh » et les collectivités de la région Bretagne sont scannés à notre initiative. Toutes autres entités désirant jouir de ce service peuvent en faire la demande auprès de Breizh Cyber.

Ce service est exécuté de la manière suivante :

- Identification des noms de domaines cibles ;
- Scan des services hébergés sur ces domaines (et sous-domaines) et exposés sur internet ;
- Première communication auprès des entités concernées par une vulnérabilité (sans aucun détails) ;
- Après prise de contact par l'entité concernée, transmission du rapport de scan détaillant la/les vulnérabilité(s) et les recommandations associées ;

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

- Suivi de la remédiation.

5.3 Recherche en source ouverte

Dans le cadre du suivi des incidents et de communication aux victimes de fuites d'informations, notamment des cas de rançongiciels, les analystes de Breizh Cyber mènent une veille en source ouverte (dark web, deep web), particulièrement sur les blogs et forums des attaquants identifiés lors de l'investigation.

6. Formulaire de notification d'incident

Un formulaire permettant de notifier Breizh Cyber d'incidents a été développé.

Les éléments suivants sont indispensables 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 ;
- Description succincte de l'incident et impact général sur l'organisation.

Les éléments suivants sont si possibles à fournir :

- Chronologie de l'incident : date et heure du début de l'incident et de sa détection ;
- Description de l'incident comprenant notamment la nature de l'incident, l'impact sur l'organisation et le nombre et type de machines touchées ;
- Actions effectuées depuis la détection de l'incident ;
- Tout 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, Breizh Cyber n'assume aucune responsabilité pour les erreurs ou omissions, ou pour les dommages résultant de l'utilisation des informations contenues.