RFC2350

CSIRT APIXIT

APIXIT
GROUPE BECHTLE

Date :
20/01/24

Classification :
TLP : CLEAR

Version :
1.0

CSIRT APIXIT
Espace Jacques Cartier
35360 Montauban de Bretagne
https://www.apixit.fr

TABLE DES MATIERES

1. A PROPOS DE CE DOCUMENT

Ce document contient une description de la cellule de veille et de réponse à incident d'APIXIT, le CSIRT APIXIT, tel que préconisé par la RFC2350.
Il fournit les informations essentielles sur le CSIRT APIXIT, ses responsabilités et les services fournis.

1.1. Date de dernière mise à jour

- V0.1 : 09/01/2025

1.2. Liste de diffusion des notifications

Il n'existe pas de liste de diffusion pour les modifications de ce document.

1.3. Lieu de distribution de ce document

La version courante de ce document est disponible sur le portail d'information du CSIRT APIXIT :
https://www.apixit.fr/csirt-apixit-une-reponse-agile-et-efficace-aux-incidents-cyber/

1.4. Authenticité de ce document

Ce document a été signé avec la clé PGP du CSIRT APIXIT.
La clé publique du CSIRT APIXIT est disponible sur le site Web du CSIRT APIXIT au lien suivant :
https://www.apixit.fr/csirt-apixit-une-reponse-agile-et-efficace-aux-incidents-cyber/

2. INFORMATIONS

2.1. Nom de l'entité

Nom complet : CSIRT APIXIT

2.2. Adresse

CSIRT APIXIT
Agence de Montauban de Bretagne
Espace Jacque Cartier, 35360 Montauban de Bretagne
France

2.3. Zone de temps

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

2.4. Numéro de téléphone

Communiqué dans le cadre du contrat de service.

2.5. Numéro de fax

Sans objet.

2.6. Autre moyen de contact

Sans objet.

2.7. Adresse électronique

Si vous devez informer le CSIRT APIXIT d'un incident de cybersécurité ou d'un acte de Cybermalveillance, veuillez le contacter à : csirt@apixit.fr.

2.8. Clé publique et information sur le chiffrement

Le CSIRT APIXIT a une clé PGP :

- Identifiant de clé : 0730 B413 1650 D57A
- Empreinte : 817A 1A29 B18B 1D3B DC5B 07B2 0730 B413 1650 D57A

https://www.apixit.fr/csirt-apixit-une-reponse-agile-et-efficace-aux-incidents-cyber/

2.9. Membres de l'équipe

La liste des membres de l'équipe n'est pas publiée. Elle est constituée d'experts en sécurité des systèmes d'information : analyse des vulnérabilités et de codes malveillants, investigations numériques (forensique) et tests d'intrusion. L'identité de l'un des membres du CSIRT APIXIT peut être communiquée au cas par cas selon la règle du besoin d'en connaitre.

2.10. Autres informations

Des compléments d'information sur le CSIRT APIXIT sont disponibles sur le portail https://www.apixit.fr/csirt-apixit-une-reponse-agile-et-efficace-aux-incidents-cyber/

2.11. Point de contact

Pour toute demande concernant la déclaration des incidents de cybersécurité, le canal de communication à privilégier pour contacter le CSIRT APIXIT est d'envoyer un email à l'adresse csirt@apixit.fr.
Le numéro d'urgence est réservé aux clients ayant souscrits au service et est communiqué dans la convention de service associée.
Le CSIRT APIXIT assure une permanence de son service de réponse à incident en 24h/24 et 7j/7.
Les interventions se font en HO et J+1.

3. CHARTE

3.1. Ordre de mission

Le CSIRT APIXIT est la cellule d'escalade et d'intervention en cas d'incidents de sécurité avérés majeurs.
Sa mission est d'accompagner ses clients dans la compréhension de l'incident, l'endiguement et la remédiation à court terme.
Elle intègre également le durcissement et l'amélioration de la sécurisation du SI avec priorisation dans la continuité du traitement de l'attaque.

3.2. Entités bénéficiant du service

La société APIXIT et ses clients peuvent bénéficier des services du CSIRT APIXIT.

3.3. Support et/ou relations

Le CSIRT APIXIT fait partie de la société APIXIT.
Elle dispose d'un canal d'échange avec l'ANSSI au travers de sa qualification PASSI.

3.4. Autorité

Le CSIRT APIXIT réalise ses activités sous l'autorité de la Direction de la société APIXIT.

4. POLITIQUES

4.1. Types d'incidents et niveau d'intervention

Le CSIRT APIXIT est la cellule d'escalade et d'intervention pour les incidents de sécurité du numérique de la société APIXIT et de ses clients.
L'appui apporté à la structure par le CSIRT APIXIT dépend du type et de la gravité de l'incident.
Dans le cas d'un nombre important d'incidents à gérer, une priorisation du traitement sera effectuée en fonction de la criticité de la menace de cybersécurité et de son impact avéré ou potentiel sur les systèmes de production.
Le périmètre du service CSIRT APIXIT est le suivant :

- Qualification de la réponse à incident réalisée en 24h/24 et 7j/7 ;
- Intervention en HO/JO :
    - Investigation numérique ;
    - Analyse de codes malveillants ;
    - Information de sécurité et alertes ;
    - Réception et analyse des déclarations d'incidents de sécurité ;
    - Appui à la réponse aux incidents ;
    - Coordination de la réponse aux incidents ;

Le service CSIRT peut participer aux services complémentaires APIXIT (avec les équipes audit et SOC) suivants :

- Veille et bulletins d'information ;
- Audit et conseil en sécurité.

Afin de garantir la disponibilité du service CSIRT, Les clients peuvent bénéficier du support d'un partenaire contractuel d'APIXIT en cas de débordement.

Le CSIRT APIXIT s'inscrit dans une démarche d'intégration à l'InterCERT France pour bénéficier d'un partage d'information sur les menaces et également pour le support des autres adhérents (CERT-FR notamment).
Le CSIRT APIXIT s'inscrit également dans une démarche de qualification PRIS avec un dépôt de dossier en 2025.

4.2. Coopération, interaction et divulgation d'informations

Les informations relatives à l'incident, telles que les noms et les détails techniques, ne sont pas publiées sans l'accord des parties prenantes concernées.
Sauf accord contraire, les informations fournies restent confidentielles.
Le CSIRT APIXIT ne transmettra jamais d'informations à des tiers sauf si la loi l'exige.
Par conséquent, ces informations peuvent être transmises à des entités telles que :

- Des experts techniques propres à l'ANSSI ;
- Les partenaires et autres parties prenantes identifiés dans la convention de services ;

- Les forces de l'ordre françaises (si la loi l'exige ou sur demande de la source d'information) ;

Le CSIRT APIXIT peut être amené à communiquer des informations au CERT-FR ou son partenaire lorsqu'il sollicite leur appui ou lorsque cela concerne une structure référencée comme OIV ou OSE.
Les informations seront transmises en fonction de leurs marquages TLP et du principe de « besoin d'en connaitre ».
Aucune information sensible ne sera envoyée par le CSIRT APIXIT à une autre partie sans un accord préalable du propriétaire de l'information.
Les informations sont gérées par le CSIRT APIXIT dans le respect du référentiel PRIS de l'ANSSI et des marqueurs TLP/PAP.

4.3. Communication et authentification

Le moyen de communication privilégié est la messagerie électronique.
Les informations sensibles sont chiffrées, à l'aide de PGP ou de Zed!, avant d'être transmises afin de garantir la confidentialité et l'intégrité des documents échangés.
PGP pourra également être utilisé pour authentifier les fichiers échangés ainsi que les messages électroniques.

5. SERVICES

5.1. Activités principales du CSIRT

5.1.1. Réponse aux incidents

L'accompagnement et l'appui mis en place par le CSIRT APIXIT dans le cadre de leur signalement consistent à :

- Récupérer le signalement de nos clients, évaluer et qualifier l'incident ;
- Proposer une posture de réponse à incident ;
- Proposer des mesures d'aide au traitement des incidents, formuler des recommandations et notamment proposer des mesures d'urgence pour limiter l'impact de celui-ci, des mesures de remédiation ainsi que des mesures destinées à améliorer la sécurité du ou des systèmes d'information concernés.

5.1.2. Triage

Les actions pouvant être réalisées sont les suivantes :

- Collecter les éléments pertinents dans le cadre du traitement de l'incident ;
- Analyser et qualifier les incidents ;
- Diffuser une alerte vers les autorités compétentes de l'Etat selon la nature de l'incident :
  - A l'ANSSI (CERT-FR) 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. Coordination

Les actions pouvant être réalisées sont les suivantes :

- Accompagner nos clients dans le traitement de l'incident de sécurité des systèmes d'information ;
- Catégoriser les informations liées à l'incident (fichiers journaux, contacts, etc.) au regard de la politique de divulgation de l'information ;
- Escalader au management APIXIT pour la mise en place d'une coordination de plusieurs services dans le cadre d'une remédiation nécessitant des compétences transverses ;
- Notifier les autres parties impliquées en cas de besoin d'en connaître, conformément aux politiques de divulgation d'informations.

5.1.4. Résolution

Les actions pouvant être réalisées sont les suivantes :

- Conseiller nos clients sur les mesures appropriées ;
- Suivre le processus de résolution des incidents ;
- Analyser des artefacts et systèmes compromis ;

- Identifier l'origine de l'incident et les mesures de remédiation associées afin d'éliminer la persistance de l'attaquant sur le SI et empêcher son retour via une nouvelle exploitation des vulnérabilités qui ont permis l'intrusion ;
- Assister nos clients durant les mesures de remédiation.

5.2. Activités complémentaires au service CSIRT

5.2.1. Veille sécurité

Les services proposés aux clients SOC APIXIT sont les suivants :

- La détection et la réaction aux incidents de sécurité afin de détecter les attaques ;
- L'information en cas d'alerte de sécurité issue d'un bulletin de sécurité.

Au-delà des services proposés, le SOC APIXIT alerte les services internes qui disposent de contacts permettant d'alerter par message électronique leurs clients concernés par une exploitation potentielle.

5.2.2. Gouvernance et Audit en sécurité

Les équipes de gouvernance SSI d'APIXIT sont en mesure de :

- Accompagner les clients dans leurs définitions de stratégies de sécurité et notamment dans la mise en place d'une politique de gestion de crise et dans les modes opératoires associés aux scénarios de risques redoutés ;
- Sensibiliser nos clients au travers d'exercices (phishing, etc.) ou de communications internes (newsletters).

Les équipes audit d'APIXIT peuvent réaliser des audits d'exposition externe aux attaques (EASM) intégrant les activités suivantes :

- Recherche de fuites de données (fuite de code-sources, fuite de données utilisateur, etc.) et évaluation de leur pertinence ;
- Réalisation d'une cartographie des machines exposées (technologies et serveurs utilisés, configuration TLS, mise à jour corrective, etc.) afin de déterminer la surface d'attaque ;
- Recherche des vulnérabilités (machines non gérées type « Shadow IT » ou serveurs mal configurés), identifiants faibles/par défaut, vulnérabilités Web (Injections SQL, XSS, LFI, RFI, etc.) et évaluation de leur exploitabilité.

A l'issue de l'audit, APIXIT délivre un rapport destiné à la direction et au responsable de la cybersécurité.
Il présente :

- Les vulnérabilités identifiées et leur niveau de criticité ;
- Les impacts en cas d'exploitation ;
- Les recommandations visant à réduire les risques identifiés.

6. FORMULAIRE DE NOTIFICATION D'INCIDENTS

Afin de faciliter la qualification de l'incident, un formulaire de déclaration d'incident de sécurité des systèmes d'information est disponible au téléchargement ici :
https://www.apixit.fr/csirt-apixit-une-reponse-agile-et-efficace-aux-incidents-cyber/
L'accès au formulaire de déclaration ne nécessite pas d'authentification préalable, il faut ensuite l'envoyer à l'adresse suivante : csirt@apixit.fr
APIXIT recommande de sécuriser cet envoi à l'aide de PGP.

7. DECHARGE DE RESPONSABILITE

Bien que toutes les précautions soient prises dans les recommandations faites par le CSIRT APIXIT, ce dernier ne peut pas être tenu responsable :

- Des impacts dès lors que les informations communiquées par le client sont erronées ou incomplètes ;
- De perturbations de la production lors de l'application de patchs ou de correctifs dans le domaine de responsabilité du client ;
- Des dommages indirects, tels que notamment le manque à gagner, la perte de clientèle, la perte de données, l'atteinte à l'image, etc. ;
- Des éventuels dommages causés par le non-respect des obligations du client (non-respect des délais, absence de sauvegarde, etc.) ;
- Des dommages causés par une personne malveillante à l'encontre du client ou des tierces parties au cours ou après la prestation.