RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CERT-FR

RETEX SUR LES APPLICATIONS SENSIBLES – VIOLATIONS DE DONNÉES

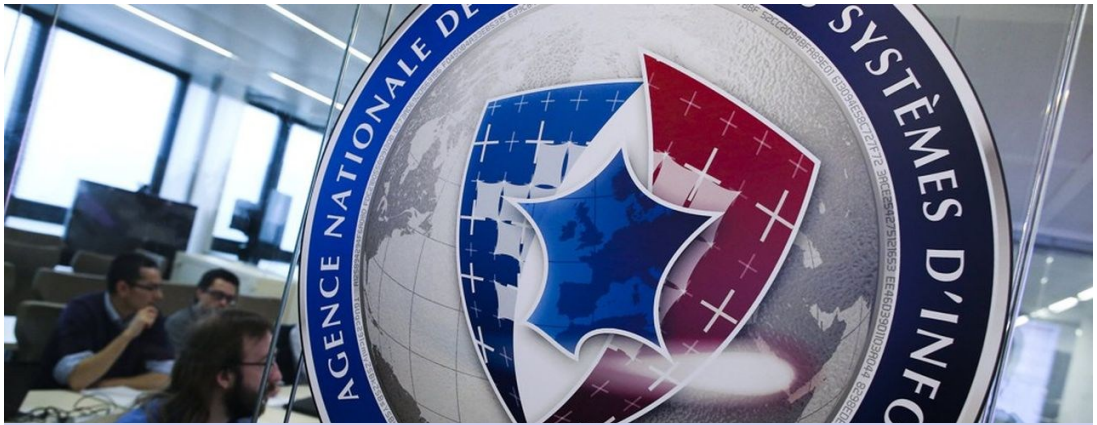
1. PRÉSENTATION

Qui sommes nous

Les intervenants

David QUESADA

Christophe RENARD



ANSSI / CERT-FR
Bureau Appui à la Reprise de Contrôle

Qui sommes nous ?

Traitement d'incidents à l'ANSSI

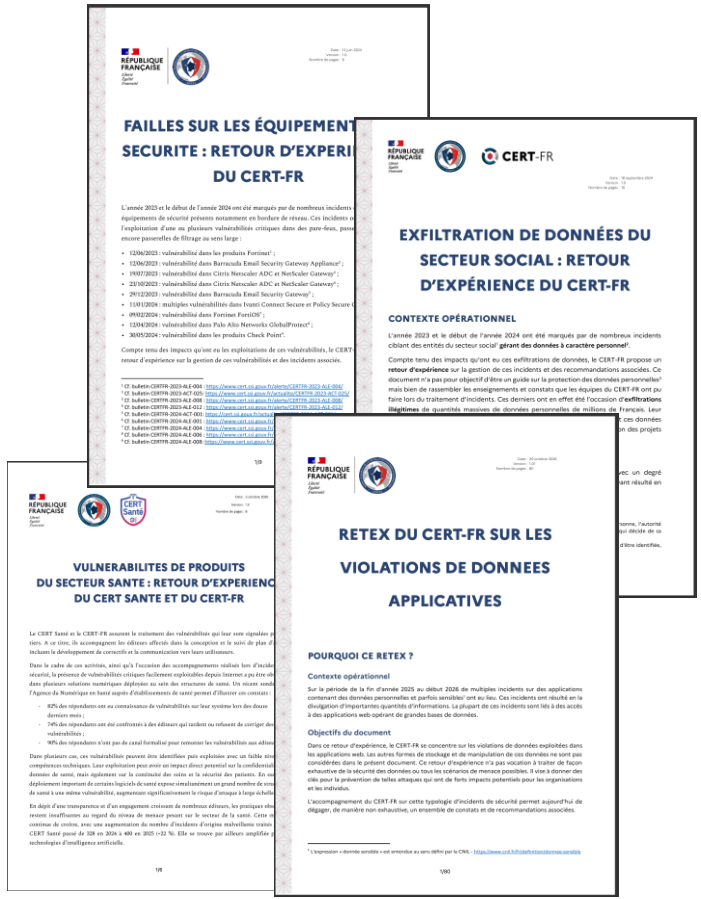
- **CERT-FR / Sous Direction Opérations**
  - Une activité constante
    - ~1000 incidents suivis par an
    - Une vingtaine d'opérations
  - Victimes allant de l'OIV
    - À la PME sensible
    - En passant par les ministères
  - Majoritairement de l'espionnage
    - Mais aussi de la cybercriminalité
    - Et tous les incidents hors normes
  - Un acteur intégré à l'écosystème
    - En suivi sur la plupart des incidents
    - Traitement par des PRIS ou équivalents
    - Et toujours en collaboration avec les victimes et leurs sous-traitants



RETEX CERT-FR

- Productions spécifiques du CERT-FR
- Basées sur nos expériences de traitement d'incident
- Pas à vocation normative
- Volonté de faire bénéficier l'écosystème de ce que nous avons appris
- Souvent des mesures basiques ⇨ mais peu mises en œuvre

CERT-FR



Ce que nous n’aborderons pas…

- Il n’y aura pas de détails sur les incidents récents et en cours.
- Les incidents REACTIV, DGFIP, ANTS, France Travail … sont dans le RETEX, mais pas que, il n’y aura pas d’information précise.
- Les investigations et la gestion de crise ne seront pas présentées.



2. SITUATION & CONSTATS

2. SITUATION & CONSTATS

3. PROJET DU DOCUMENT

4. LES 10 PRINCIPES PROPOSES

1. Situation & Constats : les incidents 1/4

Sur la période de la fin d'année 2025 depuis début 2026, de multiples incidents sur des applications contenant des données personnelles et sensibles ont eu lieu.

En 2025, le CERT-FR a été informé de **196 incidents** relatifs à des exfiltrations de données. En comparaison, **130 incidents** de ce type avaient été traités par le CERT-FR en 2024. Au *1er août 2026, plus de 170 incidents* de ce types ont été portés à notre connaissance.

Le CERT-FR **ne constate pas de ciblage particulier** : tout type de secteur et d'entité peut être victime de ce type d'incident.

Violations d'information très médiatisées et pas de guide ANSSI sur le sujet.

2. Situation & Constats : les attaques

La plupart de ces incidents sont liés à des accès à des applications web opérant de grandes bases de données avec **des identifiants et mots de passe valides**, peu d'exploitation de vulnérabilité.

Dans de nombreux cas, ces exfiltrations ont été permises par des actions attaquantes présentant **un faible niveau de complexité**.

Utilisation et réutilisation des informations venant des *Infostealers*.

2. Situation & Constats : les cibles

Nos assistances ont fait ressortir des constats récurrents:

- Authentification obsolète (login/mot de passe ou MFA faible)
- Architectures inefficientes en terme de sécurité
- Gestion d’accès internes aux applications insuffisante
- Supervision faible voire inexistante
- Menace forte, permanente, persistante, industrialisée

La réalité est très différente des publicités

2. Situation & Constats: sous-estimation 4/4

Préalablement à la mise en œuvre du RGPD, seul un sous-ensemble restreint d'informations personnelles a été traité comme sensible par de nombreux opérateurs d'application.

Les **remplacements** d'applications structurantes sont **lents,** autant dans les organisations **privées** que **publiques**.

En 2026, les attaquants peuvent encore trouver des applications où des mesures de sécurité sont anciennes et non proportionnées au niveau de la menace.

Des compromission de masse sur des données.

3. PROJET DU DOCUMENT

3. Projet du document : pourquoi ?

L'effet recherché

- **Sortir de la paralysie** : mêmes des applications *legacy* peuvent être tirées vers le haut.
- **Offrir des options pragmatiques** : ne réclamant pas de projet ou d'investissement long ou des refontes, mais plutôt de la reconfiguration.
- **Ne visant pas le haut du niveau de la menace** : la plupart des applications concernées n'ont pas une portée stratégique et ne justifient pas un investissement sécurité haut de gamme.
- **Un outil pratique** : utilisable concrètement et rapidement.

Sortir de la zone d'humiliation avant de viser plus haut.

3. Projet du document : périmètre

Tous les risques possibles sur un système d'information ne sont pas pris en compte dans les recommandations du document.

Seuls sont considérés **les risques relatifs aux violations de données dans un environnement applicatif**.

En particulier, les risques de violations de données lors de leur manipulation au sein d'un système d'information bureautique ou de développement ne sont pas considérés dans le présent document.

On ne parle que d'applications web, c'est-à-dire la plupart des applications.

3. Projet du document : risques

Les deux principaux risques considérés sont :

- **Les divulgations unitaires de données à fort enjeu** : pouvant occasionner unitairement des torts importants (possesseur d'objets de valeur, information de santé, intervenant d'une procédure judiciaire, information familiale de profession à risque…).

- **Les violations massifs de données personnelles** : pouvant occasionner des dommages moins importants - ou moins immédiats - mais à un grand nombre de personnes. Ces violations de masse viennent nourrir des campagnes de fraudes appuyées sur des informations précises et personnalisées.

Des scénarios d'attaques observées, pas de la spéculation.

3. Projet du document : scénarios de menace

Les scénarios de compromission considérés :

- **Usurpation d'identifiants** : des identifiants utilisateurs légitimes sont utilisés par l'attaquant.
- **Accès direct aux données** : une erreur de configuration expose des accès aux services ou aux données sans passer par l'application.
- **Accès par un collaborateur interne malveillant (*insider*)** : plusieurs incidents récents ont vu des utilisateurs légitimes être la source de violation de données.
- **Exploitation de vulnérabilité applicative** : des erreurs dans l'application permettent de contourner les mesures de sécurité et d'accéder illégitimement aux informations.

Des scénarios d'attaques observées, pas de la spéculation.

4. CONTENU

3. Contenu: structure

La structure du document a été pensées pour tous les acteurs :

- **Principes et scénarios** :
  - Présenter des scénarios réels et réalistes
- **Détails et explications de chaque principe** :
  - Proposer des niveaux d'explication adaptés à chaque population
- **Exemples concrets par principe** :
  - Offrir des pistes concrète d'implémentation

Du CODIR aux administrateurs en passant par les RSSI et DSI

3. Contenu: 10 principes

PRINCIPES APPLICABLES À TOUTES LES APPLICATIONS WEB GÉRANT DES DONNÉES SENSIBLES :

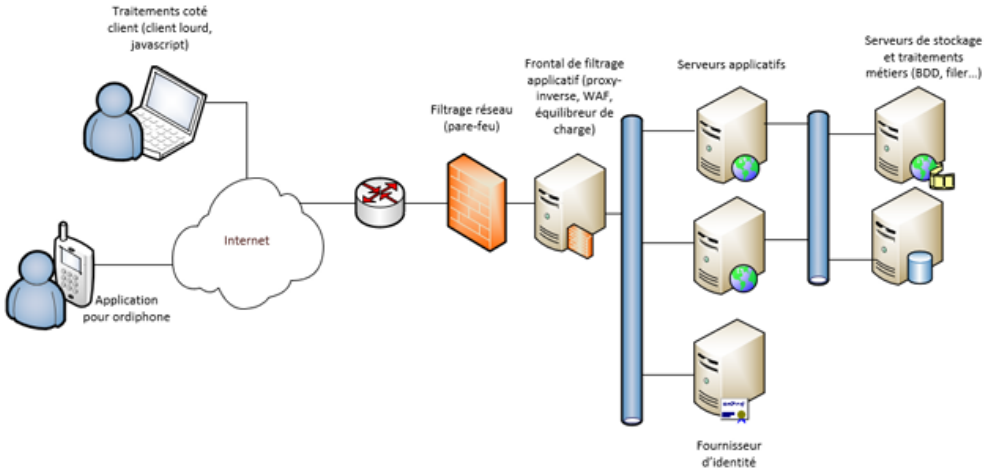
1. Appliquer une politique de gestion des données.
2. Limiter les accès utilisateurs.
3. Limiter l'exposition.
4. Dépasser le login / mot de passe.
5. Sécuriser l'environnement d'hébergement de l'application, opérer dans un environnement conforme aux recommandations des guides de l'ANSSI.
6. Tracer les actions des utilisateurs, être capable d'attribuer toute action dans l'application à un utilisateur et une adresse réseau au travers de tous les composants et sur toutes les parties de l'applications.
7. Superviser les journaux pour des traces d'anomalies, au minimum pratiquer des inspections périodiques.
8. Les situations anormales doivent déclencher des réactions automatiques et des alertes.
9. La sécurité de l'application doit être vérifiée.

PRINCIPE SPÉCIFIQUE AUX ADMINISTRATIONS :

10. Mettre en œuvre une démarche d'homologation pour chaque application conformément au Référentiel Général de Sécurité et à la Politique de Sécurité des Systèmes d'Information de l'Etat.

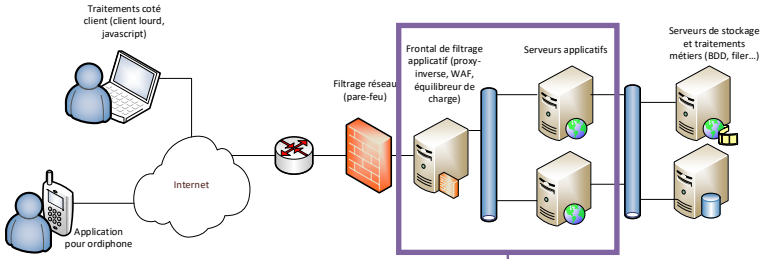
3. Contenu: la matière

Proposer des actions concrètes face aux problèmes techniques rencontrés.



Une architecture d'application web « archétypale et moderne ».

3. Contenu: principe de zoom



Un besoin : « Transmettre l'adresse IP source »

Des **exemples** de configuration :

« X-Forwarded-For » avec Nginx

```
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header Host $host;
```

« X-Forwarded-For » avec Haproxy

```
option forwardfor
```

Ne pas être exhaustifs : des constats et des « trucs et astuces ».

4. FOCUS AUTHENTIFICATION

3. Focus authentification

1. Le login mot de passe est mort

Infostealer & Login / Mot de passe :

- L'assurance de passer tous les contrôles et toute l'architecture facilement

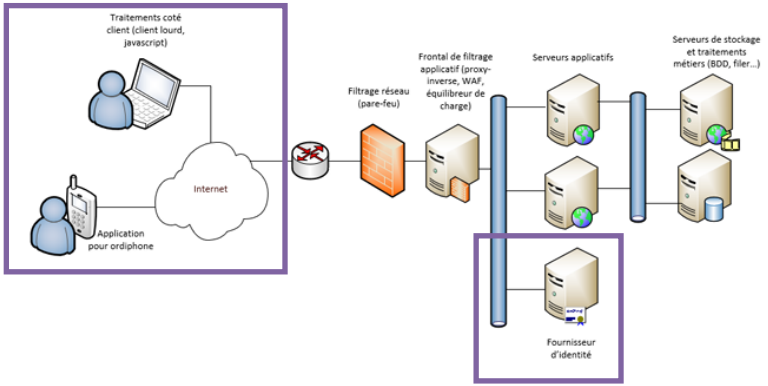
MFA mieux, mais :

- OTP saisi vulnérable au hameçonnage ciblé
- Certificats TLS Logiciel à la portée des infostealer

Le physique, la clef du succès :

- Puce TPM (passkey)
- Carte à puce, jeton FIDO2
- Application sur support physique distinct

Aucune solution ne résiste à la compromission intéractive du poste utilisateur.



À éviter

OTP SMS : Grand public pourquoi pas, le risque est le SIM-swapping des eSIM

OTP Mail : A oublier sans une messagerie protégée par un 2FA

3. Focus authentification

2. Authentification forte ce n'est pas que multi-facteur

Notifier la clef pour alerter :

- Toujours notifier une connexion pour alerter d'une possible compromission

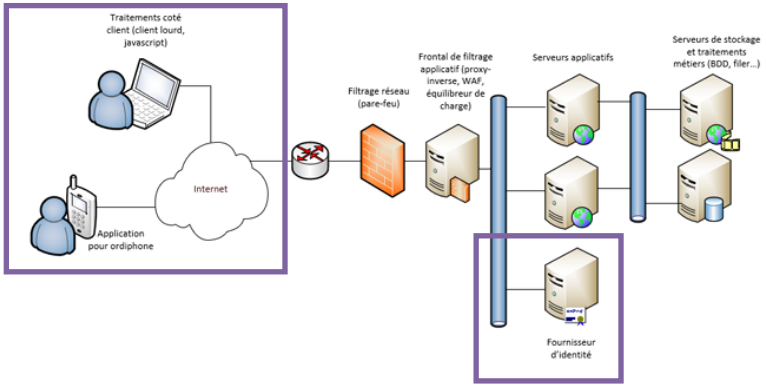
Un sous-domaine d'administration :

- Un admin.monsite[.]local bien mieux que www.monsite[.]local/admin/
- Limite l'impact des XSS
- Limit les risques d'échappement de filtrage
- Filtrage fort et supervision augmentée

Détecter et bloquer automatiquement :

- Voyage impossible et anomalies doivent pouvoir être bloqués automatiquement

Un processus de blocage et autorisation solide à mettre en place.



À ÉVITER

Authentification forte sans journalisation

Authentification forte sans détection

Authentification forte sans réaction automatique

3. Focus authentification

3. L'OUVERTURE DE SESSION, UNIQUEMENT UN DÉBUT

L'enrôlement un point faible :

- Un enrôlement ou une réinitialisation doivent être tracés comme des évènements de sécurité

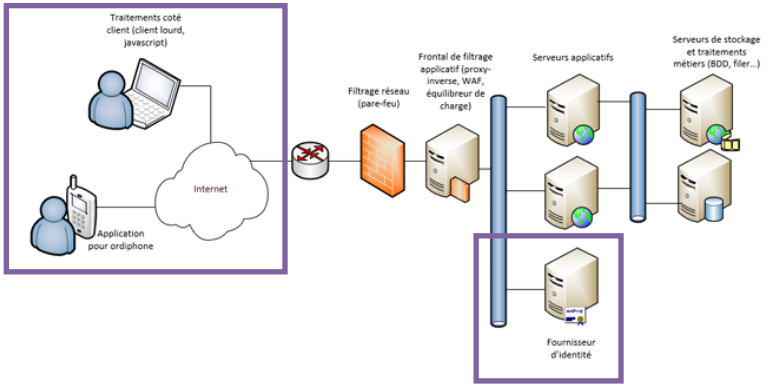
Le cookie de session vaut identité :

- HttpOnly, Secure et TLS ne protègent pas des infostealers ni des proxys malveillants
- Sessions courtes + lien IP, GéoIP, user-agent bien meilleur
- Fonctionne aussi pour des jetons d'API (OAuth par exemple)

Demain, ou aujourd'hui :

- DBSC pour les navigateurs modernes et passkeys

Ces configurations permettent la détection de comportements déviants.

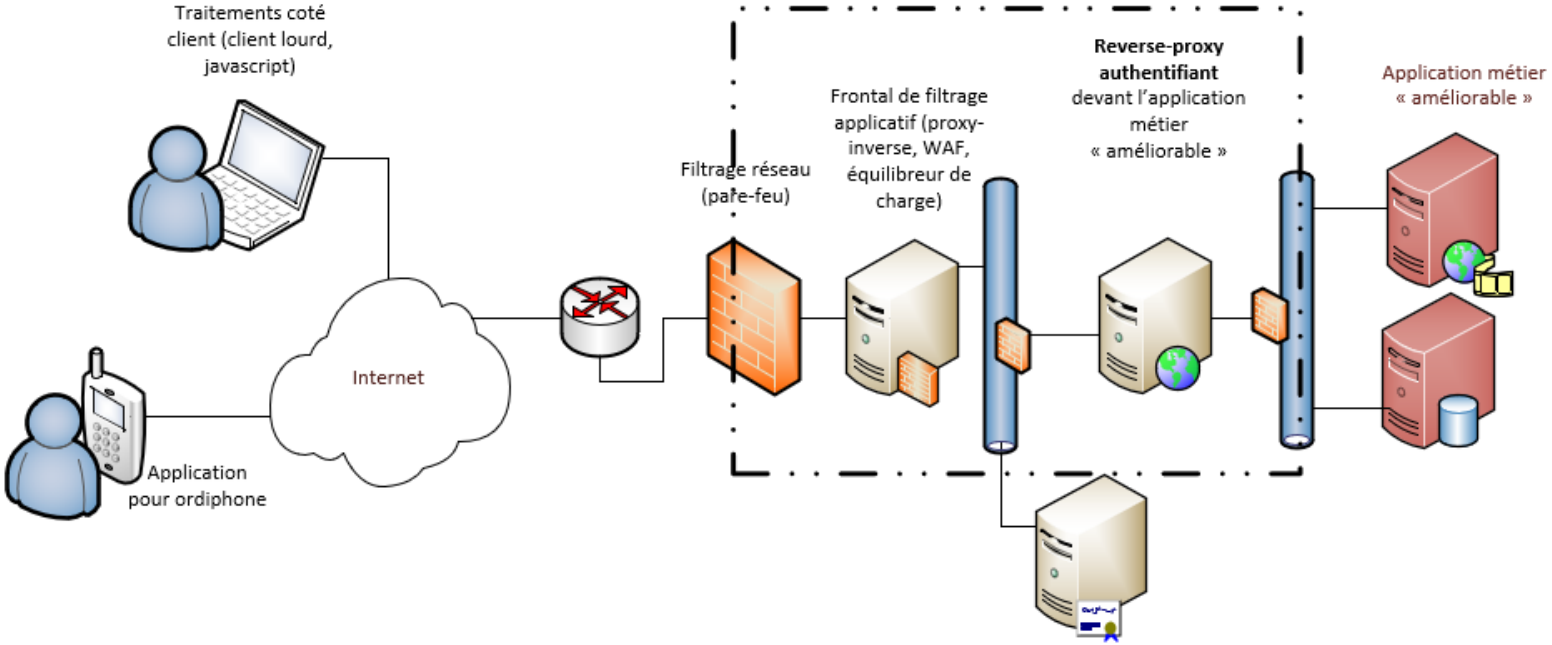


À ÉVITER

Temps de session : infini

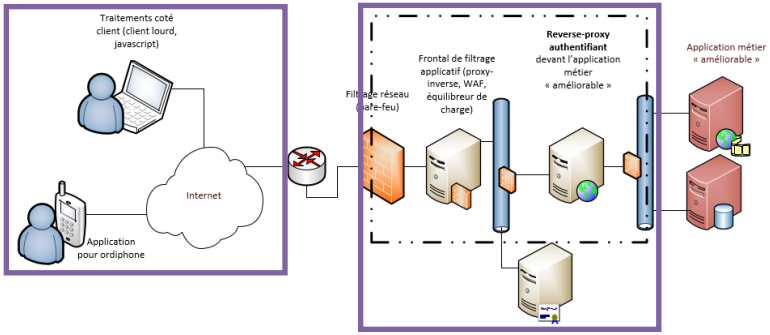
Un jeton de session « portable » entre périphériques

3. Focus authentification



Prendre l'application métier « améliorable » et la mettre dans une enclave stricte.

3. Focus authentification



4. TRANSFORMER SANS TOUT CASSER, C'EST POSSIBLE

IDP point de pivot :

- L'IDP permet de reconfigurer l'authentification en dehors de l'application
- Permet de ralentir ou bloquer

Reverse Proxy authentifiant

- Réécriture de requête transparente avec authentification sur l'IDP

Journaliser & Détecter :

- Des reverses proxy authentifiant qui journalise
- Un IDP qui journalise compte et jeton
- Les informations types IP, User-Agent … sont clefs

L'IDP est un actif de niveau 0 en mode tiering (à gérer comme tel !)

À ÉVITER

Refaire du monolithique dans l'application

Oublier le X-Forwarded-For

3. Focus authentification

Les actions d'endiguement les plus courantes sont :

- Désactiver un compte / réinitialiser un compte
- Interdire l'accès depuis une source vers une ressource
- Révoquer des certificats ou des jetons ou des sessions réseaux
- Limiter la bande passante
- Réduire l'exposition

Fiche réflexe InterCERT-France – Fuite de données : Qualification / Endiguement

Procédure d'endiguement et fiches réflexes pour les équipes IT et métiers.

4. CONCLUSION

4. Conclusion

1. Le login mot de passe c'est fini
2. L'authentification forte, ce n’est pas forcement multi-facteur
3. L'ouverture de session n'est que le début
4. La transformation peut se faire sans tout casser

4. Conclusion

Le RETEX est disponible sur le site du CERT-FR.
https://cert.cyber.gouv.fr/cti/CERTFR-2026-CTI-008/

Votre relais sera un vrai plus pour toute la communauté.

Une version 2 pourra sortir rapidement avec vos retours.
(à vos ~~crayons~~ mails)

MERCI DE VOTRE ATTENTION

DES QUESTIONS ?

Agence nationale de la sécurité des systèmes d'information – ANSSI

Retrouvez l'ANSSI sur cyber.gouv.fr