
GEBS
Atelier Cybersécurité
5 décembre 2023

PRÉAMBULE

La sécurité informatique qu'on nomme maintenant

cybersécurité est de plus en plus complexe !

Quelque soit la taille de vos entreprises,

il est important de se faire aider par des professionnels

Le risque est là !!! Nous ne sommes pas visés en particulier

*mais **les TPE/PME sont des cibles de choix***

Les aides de la Région sont là pour vous aider à

Financer nos audits cybersécurité et nos actions correctives

+ Présentation ICEB / ALEZ PC

Contenu de l'atelier

1. **La Sécurité Informatique**
   A. A quoi cela sert ?
   B. Les objectifs à atteindre.
2. **Les différents types d'attaque**
3. **Quels systèmes de protection dans ma société ?**
   A. 10 conseils : Les bons usages dans le cadre Professionnel ?
   B. Comment sécuriser son informatique ?
   C. Comment faire face ?
4. Littérature
5. Vos intervenants

I / La sécurité informatique ?

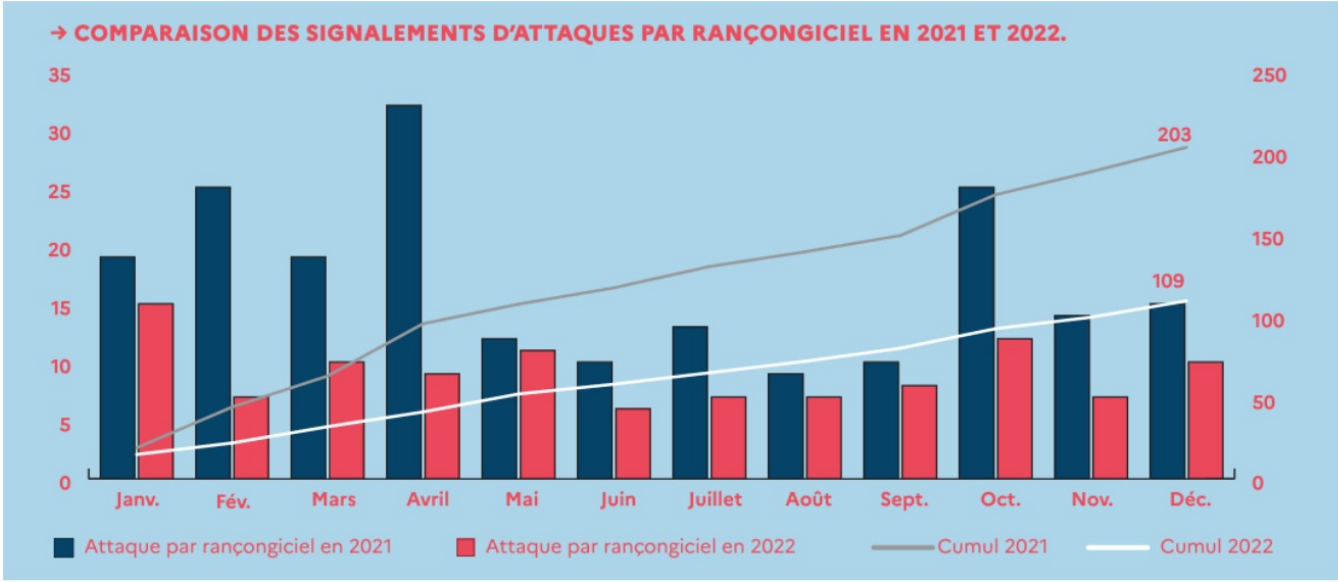
A QUOI CELA SERT ?

Elle **garantit :**

- **L'intégrité** des données
- **La confidentialité** des données
- **La disponibilité** du système
- **L'authentification** pour l'accès aux ressources

I / La sécurité informatique ?

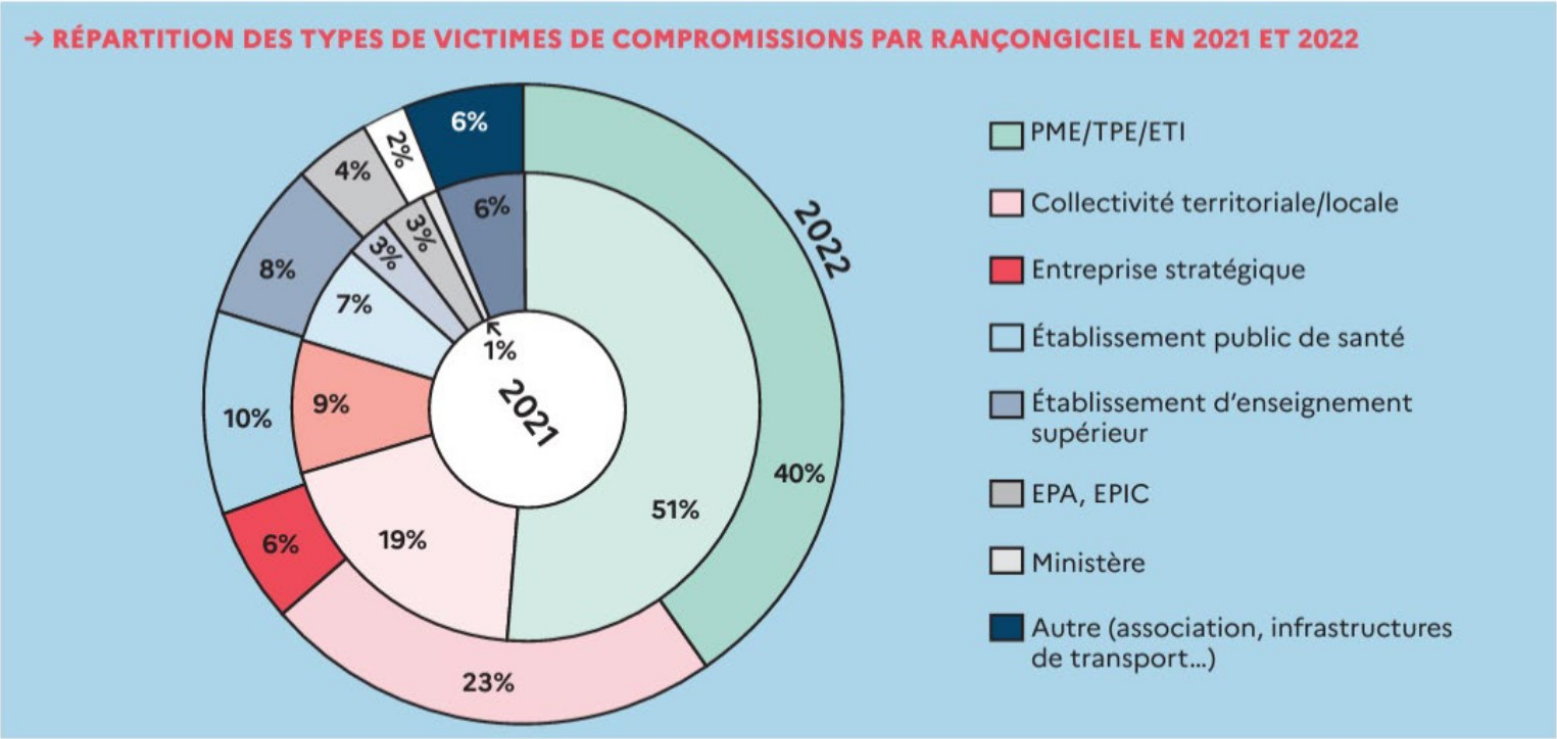
A QUOI CELA SERT ?



PANORAMA DE LA CYBERMENACE 2022 ANSSI 15

| / La sécurité informatique ?

A QUOI CELA SERT ?



I / La sécurité informatique ?

A QUOI CELA SERT ?

Garantir l'intégrité des données

Faire en sorte que les données ne soient pas altérées

COMMENT ?

→ Sauvegarde / Réplication
→ Chiffrer (https) / Signer numériquement

I / La sécurité informatique ?

A QUOI CELA SERT ?

Garantir la confidentialité/sécurité des données

S'assurer que seules les personnes autorisées aient accès aux ressources (en local, en réseau ou à distance)

COMMENT ?

→ Des utilisateurs nommés sur tous les systèmes
→ Du stockage chiffré et verrouillé (clé USB par exemple)

I / La sécurité informatique ?

SES OBJECTIFS

Garantir la disponibilité du système :
Maintenir le bon fonctionnement du système d'information
(accès à un service ou à des ressources sur site ou à distance)

COMMENT ?

→ Des solutions de redondance et des sauvegardes
→ Faire les mises à jour

I / La sécurité informatique ?

SES OBJECTIFS

Garantir l'authentification pour l'accès aux ressources

S'assurer que seules les personnes autorisées aient accès aux ressources (en local, en réseau ou à distance)

COMMENT ?

→ Mots de passe robustes / solutions de MFA

|| / Les différentes attaques

OBSERVÉES EN CE MOMENT

Le virus

Corrompt les données

Le cheval de Troie *(Trojan en anglais)*

Programme à apparence légitime (voulue) qui installe un logiciel malveillant à l'insu de l'utilisateur

Le logiciel espion *(spyware en anglais)*

Collecteur d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation, et en envoyant celles-ci à un organisme tiers

Keylogger

enregistre les frappes claviers

L'hameçonnage *(Phishing)*

L'usurpation d'identité => ATTENTION !!!

Quels systèmes de protection dans ma société ?

Bons usages & Sécurisation du SI en milieu professionnel.

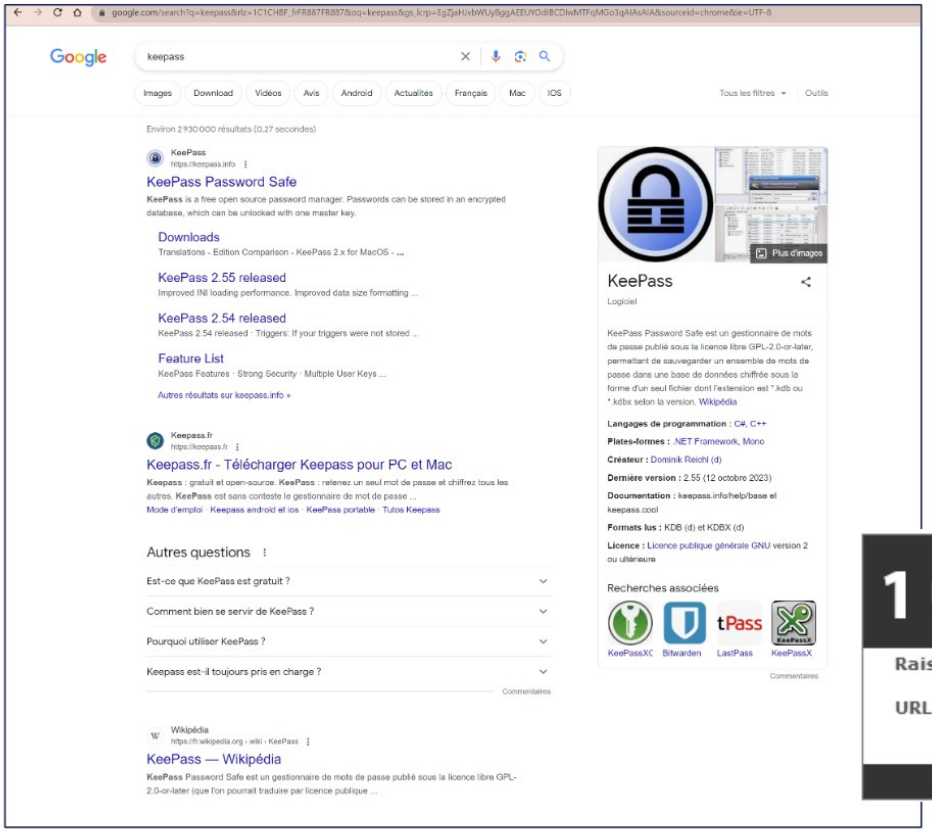
III a / Les bons usages en milieu professionnel

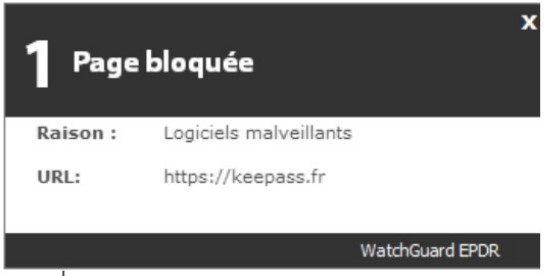
1/10 : GÉRER VOS MOTS DE PASSE AVEC SOIN

- **Utilisez un mot de passe différent pour chaque accès :** messagerie, banque en ligne, comptes de réseaux sociaux, etc. En cas de compromission de l'un de vos comptes, cela évitera l'effet boule de neige.
- **Créez un mot de passe suffisamment long, complexe et inattendu** : De 12 caractères minimum et contenant des minuscules, des majuscules, des chiffres et des caractères spéciaux.
- **Ne communiquez jamais votre mot de passe à un tiers** : Aucune organisation ou personne de confiance ne vous demandera de lui communiquer votre mot de passe.
- **Utilisez un gestionnaire de mots de passe** : Pas simple de retenir tous ses codes de connexion ! Heureusement des outils de type « coffres forts de mots de passe » existent. Ces derniers mémorisent tous vos mots de passe et vous permettent d'en générer de manière aléatoire. (Exemple : Keepass)
- https://www.economie.gouv.fr/files/bro-guide-secu-info-print_0.pdf

QUELS SYSTÈMES DE PROTECTION À METTRE EN PLACE ?

- Gérez vos mots de passe avec soin
- Recherche google
- https://keepass.fr





||| a / Les bons usages en milieu professionnel

2/10 : SAUVEGARDEZ RÉGULIÈREMENT VOS DONNÉES ET PENSEZ CHIFFREMENT

- **Effectuez des sauvegardes régulières de vos données personnelles et professionnelles sur des supports** placés en sécurité vous protège en cas de panne, de perte, de vol, de destruction de votre matériel ou d'attaque informatique. Selon vos besoins, plusieurs solutions de sauvegarde s'offrent à vous.

➔ **Ne pas confondre sauvegarde et synchronisation (exemple : OneDrive !)**

Cas n°1	Cas n°2	Cas n°3
Je suis prof libérale, auto-entrepreneur (tout est dans ma tête et mon PC/Mac !) ➔ **Sauvegarde cryptée en ligne automatique (Neobe…)**	J'ai plusieurs postes, un réseau informatique, pas de serveur local ou Cloud ➔ **Sauvegarde locale cryptée (NAS) et Cloud via Veeam Solution**	j'ai plusieurs postes, un ou plusieurs sites, un ou plusieurs serveurs ➔ **Sauvegarde locale (NAS) et redondance VPN intersites et/ou Cloud via Veeam Solution**

- **Chiffrez le contenu de vos appareils de stockage** pour éviter qu'ils ne soient attaqués avec l'aide d'un professionnel

||| a / Les bons usages en milieu professionnel

3/10 : ACCEPTEZ ET EFFECTUEZ DES MISES A JOUR RÉGULIÈRES

Un appareil ou un logiciel qui n'est pas à jour devient vulnérable et davantage exposé aux risques informatiques.

Les quelques conseils qui suivent permettent de réduire significativement ce risque.

- Identifiez l'ensemble de vos appareils et logiciels.
- Lorsque l'on vous propose une mise à jour, effectuez-la immédiatement.
- Téléchargez les mises à jour uniquement depuis les **sites officiels des éditeurs.**
- Sur vos appareils, **activez l'option de téléchargement et d'installation automatique des mises à jour** quand elle existe.

||| a / Les bons usages en milieu professionnel

4/10 : ANTIVIRUS / PARE-FEU

- **Sur Internet, les logiciels malveillants (virus, vers, cheval de Troie, logiciel espion, etc.) représentent un risque réel.** Pour vous protéger de ces intrusions, les outils suivants sont de précieux alliés.
- **Un antivirus dont vous respectez les recommandations** chaque fois qu'il vous demande de mettre à jour les bases virales ou de supprimer ou mettre en quarantaine un fichier suspect.
- **Un pare-feu bien configuré** qui bloquera les connexions non désirées depuis votre ordinateur. Pensez à l'obligation légale (1an) des stockages de logs !!!
- **L'efficacité de ces outils ne sera complète qu'à condition d'y associer quelques bonnes pratiques**. N'utilisez jamais un service ou un équipement inconnu ou abandonné (une clé USB pas exemple).

III a / Les bons usages en milieu professionnel

5/10 : WIFI

En interne

- **Séparer le wifi interne du wifi invité** (en changeant régulièrement le mot de passe)

En externe

- **Désactivez les connexions sans-fil** (Wi-Fi, Bluetooth, NFC, …) lorsque vous ne vous en servez pas pour éviter que vos appareils s'y connectent automatiquement.
- **Privilégiez la connexion privée** associée à votre abonnement mobile.
- **Si vous n'avez d'autre choix que d'utiliser un Wi-Fi public, veillez à ne jamais y réaliser d'opérations à caractère sensible** (paiement par carte bancaire, déclaration d'impôts, renseignement d'informations confidentielles, etc.) et si possible utilisez un réseau privé virtuel (VPN) - ex : solution mobile security de Fsecure

||| a / Les bons usages en milieu professionnel

6/10 : SEPARER LES USAGES PROFESSIONNELS ET PERSONNELS

- **Evitez d'utiliser vos moyens personnels** (adresse mail, téléphone mobile, clé USB, etc.) **à des fins professionnelles et inversement**.

- **Ne connectez pas d'équipements personnels, ou non fournis par votre service informatique, au réseau de votre entité ou à un équipement professionnel** (téléphone mobile personnel, clé USB ou gadget électronique offert, etc.).

- À l'inverse, ne connectez vos équipements professionnels sur votre réseau personnel que dans les conditions prévues par votre service informatique.

- **N'utilisez pas votre adresse mail professionnelle pour vous inscrire sur des sites Internet à titre personnel et réciproquement**.

||| a / Les bons usages en milieu professionnel

7/10 : DONNEZ LES BONNES PERMISSIONS / GEREZ LES UTILISATEURS

- **Bien définir les droits d'accès aux données** (fichiers, applis…) pour chaque utilisateur

- **Gérer les départs comme les arrivées** (pensez à supprimer les accès du personnel sortant)

- **Faire des niveaux de droits simples** (pas d'arborescence compliquée !!!)

→ ET CECI pour vos accès aux NAS, SERVEURS, SHAREPOINT…

Ce principe simple limite les conséquences dommageables en cas d'attaque et augmente considérablement votre sécurité numérique et facilite les sauvegardes

||| a / Les bons usages en milieu professionnel

8/10 : PROTÉGER VOTRE MESSAGERIE

- **Ne cliquez jamais sur un lien ou une pièce jointe qui vous semblent douteux.** En cas de suspicion, passez la souris sur le lien pour voir apparaître l'adresse vers laquelle il dirige et appréciez sa légitimité.
- **Ne répondez jamais à un mail suspect.** Au moindre doute, contactez l'expéditeur par un autre canal.
- **Vérifiez les paramètres de sécurité** de votre compte de messagerie.
- Si le fournisseur de messagerie le permet, **activez la double authentification pour sécuriser vos accès.** messagerie le permet, Renforcer les sécurités DKIM etc…
- **Mettez en place une sauvegarde de vos messageries** (Office365 n'est pas une sauvegarde – c'est une synchro !)
- **Mettez un antispam en place** (autofinancement !)

||| a / Les bons usages en milieu professionnel

9/10 : MAÎTRISEZ VOS INFORMATIONS DIFFUSÉES SUR INTERNET

- **Veillez également à bien identifier les personnes avec qui vous communiquez sur Internet.**

Si vous avez un doute sur une identité, contactez cette personne par un autre moyen avant d'effectuer la moindre action ou de répondre à une requête.

- **LinkedIn / Twitter / Facebook**

- **Votre site web** – formulaire de contact protégé

||| a / Les bons usages en milieu professionnel

10/10 : SE FAIRE AIDER

À partir de 3 postes :

Prendre contact avec une société de support informatique:

- **Faire réaliser un audit** axé sur la sécurité informatique
- **Documenter son réseau et l'expliquer à son personnel** (arborescence, gestion des droits)
- **Faire vérifier préventivement son parc** (comme une voiture ça se révise)
- **PROFITER des outils de MONITORING** de son prestataire
- **Avoir un seul Prestataire** - éviter que tous les dépanneurs informatiques et les copains informaticiens mettent la main sur le réseau et bidouillent vos PC ;-)

||| b / Comment sécuriser son informatique ?

COMBIEN ÇA COÛTE ?

- **ANTIVIRUS**

Entre 30 et 40 € HT par poste par an

- **ANTISPAMS**

Avec ou sans authentification (environ 45 € HT par poste par an)

- **Contrat de support IT**

A partir de 25€ HT/mois par poste

- **Sauvegarde**

NAS à partir de 300€ - Solution cloud à partir de 10€/mois

||| b / Comment sécuriser son informatique ?

COMBIEN ÇA COÛTE ?

- **FIREWALL (pare feu)**

Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit d'une passerelle filtrante comportant au minimum les interfaces réseau suivante : une interface pour le réseau à protéger (réseau interne) ; une interface pour le réseau externe.

  - filtrage
  - enregistrement des logs (obligation légale)
  - pour les + équipés : gestion des lignes internet, autorisation des accès, VPN…

De 500€ à 2500 € l'équipement

Et

De 250 € à 750 € l'abonnement annuel pour les mises à jour

||| b / Comment sécuriser son informatique ?

COMMENT FAIRE FACE ? - LOGICIELS & MATÉRIELS

- **Souscrire une assurance cyber** si votre RC ne la couvre pas

J'ai été attaqué ?

CYBERATTAQUE : PREMIERS RÉFLEXES

1. **Alertez immédiatement votre support informatique** si vous en disposez afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).
2. **Isolez les systèmes attaqués** afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.
3. **Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique…)
4. **Tenez un registre des évènements et actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.
5. **Préservez les preuves de l'attaque** : messages reçus, machines touchées, journaux de connexions…

||| b / Comment sécuriser son informatique ?

COMMENT FAIRE FACE ? - LOGICIELS & MATÉRIELS

J'ai été attaqué ?

CYBERATTAQUE : PREMIERS RÉFLEXES

6. **Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.
7. **Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager, voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle.
8. **Alertez votre banque** au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.
9. **Déposez plainte avant toute action de remédiation** en fournissant toutes les preuves en votre possession.
10. **Identifiez l'origine de l'attaque et son étendue** afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.
11. **Notifiez l'incident à la CNIL dans les 72 h** si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.
12. **Gérez votre communication pour informer** avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias...

||| b / Littérature

POUR ALLER PLUS LOIN

- https://secnumacademie.gouv.fr/
- https://cyber.gouv.fr/
- https://www.cybermalveillance.gouv.fr/
- https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles
- https://www.cert.ssi.gouv.fr/
- https://www.cnil.fr/fr/professionnel
- https://www.iledefrance.fr/aides-et-appels-a-projets/cheque-diagnostic-cyber

AVIS DE SÉCURITÉ

Les avis sont des documents faisant état de vulnérabilités et des moyens de s'en prémunir

29 novembre 2023	CERTFR-2023-AVI-0984	Multiples vulnérabilités dans les produits Axis
29 novembre 2023	CERTFR-2023-AVI-0983	Multiples vulnérabilités dans Google Chrome
29 novembre 2023	CERTFR-2023-AVI-0982	Vulnérabilité dans Apache Tomcat
29 novembre 2023	CERTFR-2023-AVI-0981	Vulnérabilité dans Joomla
27 novembre 2023	CERTFR-2023-AVI-0980	Multiples vulnérabilités dans les produits Spring
24 novembre 2023	CERTFR-2023-AVI-0979	Vulnérabilité dans les produits NetApp
24 novembre 2023	CERTFR-2023-AVI-0978	Multiples vulnérabilités dans le noyau Linux de RedHat
24 novembre 2023	CERTFR-2023-AVI-0977	Multiples vulnérabilités dans le noyau Linux de Ubuntu

VOIR TOUS LES AVIS »

|V/ Vos Intervenants

Bruno SEUX
Tél. : 01.30.15.72.76
Mail : bseux@iceb.com

INFO 3S infogérance

Valérie LIEGEARD
Tél. : 01.30.15.15.50
Mail : valerie.liegeard@alezpc.fr

Alez PC

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

En cours d'obtention

Merci.

N’hésitez pas à nous poser toutes vos questions.