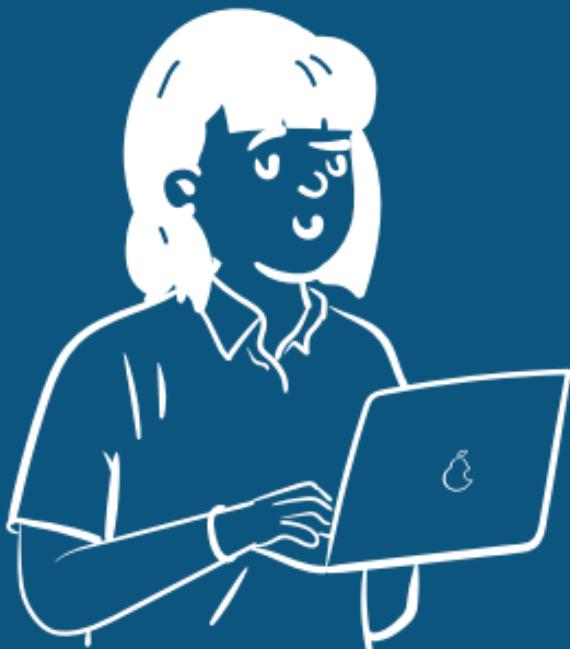


LE PETIT LIVRE DE LA CYBERSÉCURITÉ

Prévention & gestion de crise



CERT-FR 7j/7, 24h/24 au :
+33 (0)1 71 75 84 68
cert-fr@ssi.gouv.fr

En cas d'incident :



Le petit livre de la cybersécurité

Comment éviter les cyberattaques ? Que faut-il mettre en place lors d'une crise ? Le petit livre de la cybersécurité reprend pas à pas les conseils et différentes étapes à ne surtout pas rater !

Introduction	p.4
Prévenir	p.13
Se prémunir	p.21
Gérer la crise	p.27
Sortir de crise	p.35
Glossaire	p.39
Fiches pratiques	p.49
Bibliographie	p.59

Une production par



Qu'est-ce qu'une cyberattaque ?

Une cyberattaque est une tentative délibérée **d'exploiter, altérer, endommager ou détruire** des systèmes d'informations.

Elles peuvent avoir des conséquences variées, allant de la simple **perte de données à la paralysie complète**. Elles entraînent des **dommages financiers, des atteintes à la réputation et même des dommages physiques**.

43%

des PME ont constaté un incident de cybersécurité en 2020



Si le cyberrisque était un pays, il serait la **3ème économie mondiale** !

Source : La cybersécurité des entreprises – Prévenir et guérir : Quels remèdes contre les cyber virus ? – Sénat. (s. d.-b). Sénat. <https://www.senat.fr/rap/r20-678/r20-6780.html>

Est-ce que vous connaissez le coût moyen d'une violation de données en 2023 ?

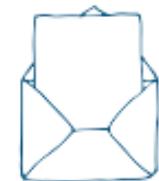


4,45m \$
soit +15% en 3 ans

Source : Coût d'une violation de données en 2023 / IBM. (s. d.). <https://www.ibm.com/fr/reports/data-breach>

Qu'est-ce qu'un système d'information ?

La première pensée que l'on pourrait avoir concernant un système d'information (SI) est qu'il s'agit de matériels informatiques. Cependant, le SI ne concerne pas seulement le système informatique. **Le SI est l'ensemble des informations !** La définition de l'information écarte notre premier *a priori* car celle-ci peut être :



transmise par courrier papier

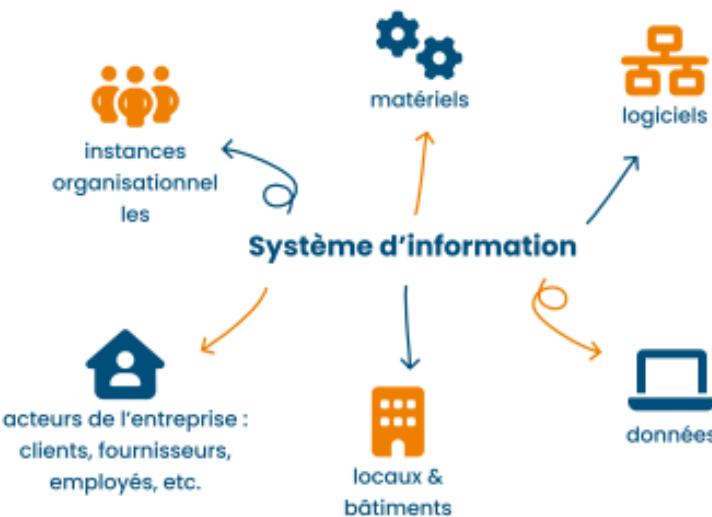


ou électronique

L'information peut même se retrouver de manière orale, par exemple : notre conversation !



Le système d'information (SI) désigne l'ensemble des moyens qui permettent de collecter, éditer, traiter, stocker, diffuser et **supprimer** de l'information.



Afin d'anticiper les différents préjudices qu'une entreprise pourrait subir en cas cyberattaque, il est vital de mettre en place une **Politique de Sécurité des Systèmes d'Information (PSSI)** pour garantir la protection du système au travers de quatre grands axes.

Ces axes sont : La disponibilité, l'intégrité, la confidentialité et la non réputation



Pourquoi protéger son système d'information ?

Les entreprises, quelles que soient leur taille ou leur secteur d'activité, dépendent de plus en plus des technologies de l'information pour mener à bien leurs opérations. Cette dépendance accrue expose ces systèmes à des menaces potentielles.

60 % des petites entreprises victimes d'une cyberattaque font **faillite dans les six mois**. La cybercriminalité coûte aux petites et moyennes entreprises plus de **2,2 millions de dollars par an**. Il y a eu une augmentation de **424%** des nouvelles cyber-violations des petites entreprises en 2019-2020.

La cybersécurité des entreprises - Prévenir et guérir : Quels remèdes contre les cyber virus ? - Sénat. (s. d.). Sénat. <https://www.senat.fr/rop/>



90%

des cyberattaques sont attribuables à des erreurs humaines

Source : EDR (Détection et réponse aux terminaux) IBM. (s. d.). <https://www.ibm.com/fr-fr/topics/edr>

Le saviez-vous : Une attaque informatique est généralement furtive



Mais quelles conséquences ?

Matérielles

Dommages et destruction de biens. Pertes de données et de travaux.

Réputationnelles

Impact sur l'image et la notoriété de l'entreprise.

Corporelles

Risques pour la santé physique, le bien-être (stress, anxiété, dépression) et la sécurité des employés.

Productivité

Interruption des opérations, retards. La perte de données peut aussi entraîner une perte du travail réalisé.

Financières

Perte de chiffre d'affaires, sanctions, implications avec la Direction Générale des Finances Publiques (DGFiP) et augmentation des coûts d'assurance.

Juridiques

Responsabilité pénale ou civile et perte de la propriété intellectuelle.

Environnementales

Dégâts physiques sur des infrastructures provoquant des catastrophes.

Qu'en est-il du RGPD ?

Le **Règlement Général sur la Protection des Données** (RGPD) est une réglementation de l'**Union Européenne** visant à renforcer la protection des données personnelles, il ne protège cependant pas des attaques. Entré en vigueur en **2018**, il impose des règles strictes sur la collecte, le traitement et la sécurité des données tout en accordant aux individus un plus grand contrôle de l'utilisation qui peut être faite des données les concernant.



**En cas de non-respect
de ces règles :**

Grandes entreprises

Amende équivalente à **4%**
du chiffre d'affaires
annuel mondial.

TPE & PME

Amende jusqu'à **20M**
d'euros

L'article 32 du RGPD impose une **obligation** de sécurité du traitement des **données personnelles**.

En plus de tout ça, certaines entreprises doivent appliquer la directive européenne **NIS 2**

(La Directive NIS 2 / ANSSI (s. d.).
<https://cyber.gouv.fr/la-directive-nis-2>



Quelles responsabilités pour le chef d'entreprise ?



En tant que chef d'entreprise, je risque jusqu'à 5 ans d'emprisonnement et 300 000€ d'amende ...

Mais que me reproche-t-on ?

Une négligence et une insuffisance de préparation de l'entreprise.

Un manquement à l'obligation d'assurer la sécurité des données.

Un défaut de notification de la violation de données aux autorités de contrôle et aux personnes concernées.

Les **actionnaires**, les **autres dirigeants**, les **autorités de contrôle** et le **Ministère public** sont susceptibles de déclencher des procédures judiciaires pour ces manquements ...

Quels sont les différents types de cyberattaques et quels sont leurs buts ?



Quelques explications :



Les malwares, le phishing, les spywares et keyloggers, les attaques sur les mots de passe, ou de force brute, le spearphishing, le vishing et les virus sont des cyberattaques qui vont cibler directement l'ordinateur ou le serveur. Ils sont connus pour restreindre l'accès au système d'exploitation, voler des données personnelles ou porter atteinte au fonctionnement du système.



L'attaque Man-in-the-Middle se concentre sur l'interception de communications entre deux entités : entre l'ordinateur et un serveur quand celui-ci se connecte à un site.



Les injections de SQL et le DoS/DDoS sont des attaques qui visent à corrompre la base de données d'un serveur ou à rendre un serveur indisponible en surchargeant sa capacité de travail par de multiples requêtes.

Vous souhaitez prendre des notes ?

Vous souhaitez prendre des notes ?

PRÉVENIR

- | | | |
|---|--|------|
| 1 | Gestion des comptes utilisateurs | p.14 |
| 2 | Les 10 préconisations | p.15 |
| 3 | Sécurisation de l'ordinateur | p.17 |
| 4 | Sécuriser son téléphone | p.18 |
| 5 | Conseils généraux pour la protection personnelle | p.19 |

Gestion des comptes utilisateurs

Derrière chaque système d'information se trouve des acteurs humains : des employés, des chefs d'entreprise, des administrateurs systèmes et des prestataires.



Les comptes utilisateurs

- Vérifier que les comptes sont toujours actifs
- Vérifier les permissions données aux comptes
- Supprimer les comptes dits "fantômes" suite aux licenciements, démissions, départs.

Je m'identifie : je suis
Je m'authentifie : je le prouve



Authentification forte

- Utiliser une double authentification : un mot de passe et un autre moyen supplémentaire (SMS par exemple)



Contrôle d'accès

S'assurer qu'aucun comportement suspect n'ait lieu (activité durant les jours de repos, accès à des sites restreints, etc.)



Contrôle des comportements

Surveiller les comportements des utilisateurs dans le traitement des informations.



Gestion des mots de passe

- Sensibiliser sur la nécessité de changer régulièrement de mot de passe
- Sensibiliser sur la nécessité d'avoir un mot de passe "robuste" (complexe)
- Utiliser un gestionnaire de mots de passe labellisé par l'ANSI

Consultez notre fiche pratique sur les mots de passe en fin de livret

I. Il faut procéder à un inventaire de tous ses biens essentiels

Il faut répertorier les données essentielles de votre entreprise ainsi que les ressources nécessaires à leur traitement : documents, brevets, savoir-faire, équipements matériels et logiciels, structure du réseau, et comptes privilégiés. Cet inventaire doit être sécurisé et accessible uniquement aux personnes autorisées.

II. Surtout, ne pas oublier de sauvegarder

Il est crucial d'avoir une sauvegarde de vos données vitales en cas de crise.

Cette sauvegarde doit être :

Pertinente, automatisée, fréquente, répertoriée et identifiée (étiquetée) sur un support externe, externalisée (stockée dans un autre bâtiment), testée régulièrement

III. Il faut exiger l'authentification...

L'authentification clarifie les responsabilités et garantit la non-répudiation des actions. La gestion des mots de passe implique un suivi individuel pour chaque employé ou intervenant externe. Consultez la fiche pratique sur les mots de passe.

IV. ...Et imposer la sécurité

Pour renforcer la sécurité, il faut :

Équiper les postes de travail et les appareils nomades (téléphones, tablettes...) d'un antivirus et d'un pare-feu, s'assurer que les systèmes d'exploitation et les logiciels se mettent à jour automatiquement, protéger ces outils et leurs sessions avec des mots de passe et une mise en veille automatique sécurisée, limiter l'accès administrateur au strict minimum (pas d'accès administrateur pour le chef d'entreprise et ses collaborateurs proches), crypter les périphériques contenant des données sensibles et utiliser un VPN, installer des logiciels permettant de localiser et d'effacer à distance les données des périphériques volés.

Cette sauvegarde doit être :

Pertinente, automatisée, fréquente, répertoriée et identifiée (étiquetée) sur un support externe, externalisée (stockée dans un autre bâtiment), testée régulièrement

V. Veiller à sensibiliser l'équipe

Informez régulièrement vos collaborateurs des risques liés à l'utilisation des données de l'entreprise et du système informatique, ainsi que des nouveaux dangers tels que les e-mails et les conférences. Faites signer une charte informatique à vos collaborateurs pour définir leurs droits et responsabilités. Limitez l'utilisation d'outils informatiques personnels. Sensibilisez votre personnel à la protection des données professionnelles et aux risques liés aux e-mails, notamment ceux provenant d'expéditeurs inconnus ou contenant des liens ou des pièces jointes douteux.

VI. Être en règle

En tant que chef d'entreprise, vous êtes responsable légalement des données personnelles et de leur utilisation par vos collaborateurs. Assurez-vous de respecter les droits et obligations définis par la CNIL. Veillez à la conformité des licences logicielles et du contenu protégé par le droit d'auteur. Vous devez également faire respecter les règles légales de surveillance des employés, en tenant compte de la vie privée sur le lieu de travail.

VII. Il faut appréhender l'externalisation

Il est important d'évaluer les risques liés à l'externalisation de tout ou partie de votre système informatique, que ce soit vers le cloud, l'infogérance, ou autre. Les données hébergées aux États-Unis doivent être conformes à la réglementation Safe Harbor. Utilisez des clauses de confidentialité et formalisez vos exigences concernant l'externalisation, telles que la disponibilité, l'intégrité et la réversibilité des données en cas de résiliation de contrat, ainsi que l'effacement sécurisé.

VIII. Protéger vos locaux

Pour sécuriser votre entreprise, assurez-vous que les locaux sont protégés contre les intrusions physiques, le vol, l'espionnage industriel et d'autres actes malveillants, de jour comme de nuit. Adoptez une approche de défense en profondeur, incluant la détection, l'alerte et la prévention. Accompagnez chaque intervenant extérieur et surveillez les prestataires de services, ainsi que les zones sensibles. Sensibilisez vos collaborateurs aux risques d'intrusion et de malveillance.

IX. Savoir alerter

En cas de compromission de votre système informatique, conservez tous les éléments de preuve, isolez l'ordinateur infecté et contactez la gendarmerie locale en composant le 17. Fournissez autant de détails que possible (qui, quoi, où, quand, comment). Selon la gravité de l'incident, la gendarmerie pourra mobiliser des enquêteurs spécialisés en cybercriminalité (Ntech).

X. S'informer et rester à l'affût

Vous disposez de plusieurs sites institutionnels de référence pour entretenir vos connaissances :

www.gendarmerie.interieur.gouv.fr

www.ssi.gouv.fr

www.intelligence-economique.gouv.fr

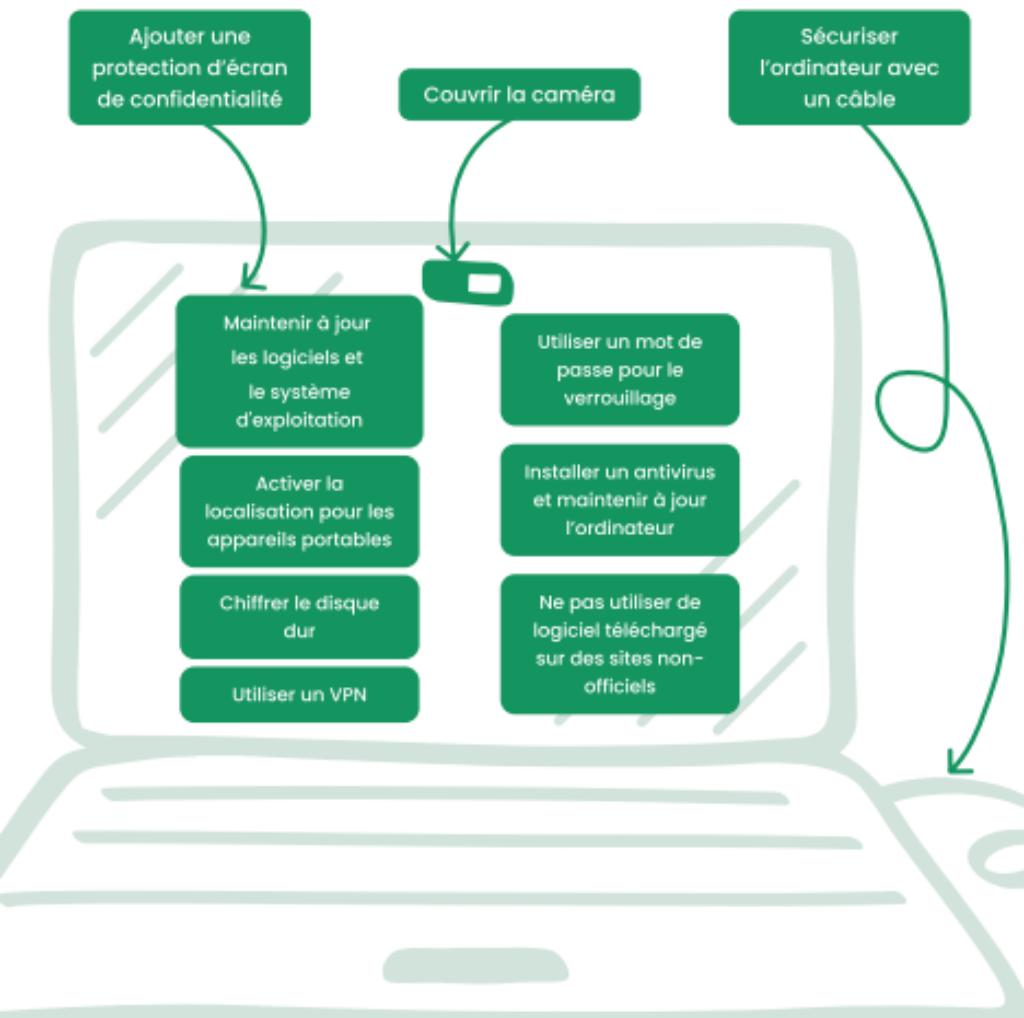
www.cnil.fr

www.internet-signalement.gouv.fr

www.signoii-spam.fr

www.phishing-initiative.com

Sécurisation de l'ordinateur



4

Sécuriser son téléphone

Configurez un verrouillage automatique

N'hébergez pas de données professionnelles sur vos équipements personnels

En cas de restauration, conservez vos contenus sur un support externe chiffré

En plus du code PIN, ajoutez un code supplémentaire sur les applications sensibles

Vérifiez les autorisations d'accès et les données concernées lors d'un téléchargement d'application

En cas de déplacement...



- Ne vous séparez jamais de vos appareils tout le long du voyage
- Sécurisez votre navigation internet en ajoutant un VPN sur votre appareil
- Gardez seulement le strict minimum de contenu sur votre appareil lorsque vous êtes à l'étranger
- Changez les mots de passe utilisés durant le voyage

Conseils généraux pour la protection personnelle



N'oubliez pas de mettre les sites web en favori pour éviter les erreurs de saisie et ...



- de vérifier les sources de vos emails

Pensez surtout à sauvegarder vos données !
Vous connaissez la règle 3, 2, 1 ?

3 copies de vos données

sur **2** supports différents de stockage

et **1** copie dans un lieu sécurisé



Vous souhaitez prendre des notes ?

SE PRÉMUNIR

1

Assurances

p.22

2

Quels outils et quelles offres pour mieux se protéger

p.23

3

Changer vos outils du quotidien

p.24

1 Assurance



Mais l'assurance cybersécurité c'est quoi ?

Elle vise à aider les entreprises à minimiser les risques financiers liés aux incidents de sécurité informatique (cyberattaques, violations de la vie privée, pertes de données, ransomwares, ...)

Quels critères ?

⌚ Respect des règles d'hygiènes

Les minimums requis sont les **12 règles de l'ANSSI**, ainsi qu'une sensibilisation des employés.

<https://cyber.gouv.fr/publications/guide-des-bonnes-pratiques-de-linformatique>

💼 Recommandé pour tous !

Pour les TPE et PME, le prix est entre **moins de 1000 euros** à quelques milliers d'euros, pour une protection qui peut en couvrir plusieurs millions !

Le contrat

⌚ Volet de prévention

Un volet pour aider à mettre en place les outils nécessaires pour se protéger des potentielles attaques.

💼 Volet de dommages

Prise en charge de certains frais pour permettre à l'entreprise de reprendre au plus vite son activité.

👤 Volet de responsabilité civile

Prise en charge en cas de violation de données sensibles ou de la vie privée et dommages psychologiques.

Quels outils et quelles offres pour mieux se protéger ?

Les entreprises ont aussi besoin de se défendre. Une attaque peut coûter beaucoup d'argent, nuire aux affaires, et mettre à mal la réputation.

Avoir recours à un professionnel pour mettre en place des solutions de sécurité informatique n'est pas aussi cher que ce que l'on croit !

SERVICE	COÛT
Antivirus	de 56 à 100 € par an
Pare-feu	démarre aux alentours de 1 000 € HT
Sauvegarde	environ 600 000 € annuels
Anti-phishing	le coup d'une attaque phishing est d'environ 100 000 €
Have I been pwned ? https://haveibeenpwned.com/	Gratuit
MonAideCyber https://beta.gouv.fr/literature/mon-aide-cyber.html	Gratuit
Di@gon@l	Anti-virus

N'hésitez pas à faire des devis !



Ces informations ne sont pas exhaustives, et peuvent changer en fonction des besoins et de vos exigences de sécurité. Cependant, il reste tout de même abordable de se protéger et de protéger son entreprise.

Données renseignées grâce à une interview d'un chef d'entreprise spécialisé en cybersécurité à Bordeaux.

Changer vos outils du quotidien

Les outils que nous utilisons au quotidien soulèvent des préoccupations quant à la récolte de nos données. Vous pouvez opter pour des alternatives afin de garantir la protection de vos données et de favoriser le développement et la souveraineté nationale.

Hootsuite

Vous pouvez utiliser Agorapulse.



WeTransfer

Vous pouvez utiliser Smash.



Whatsapp

Vous pouvez utiliser Olvid.



solution certifiée par l'ANSSI

Teams

Vous pouvez utiliser Tixeo.



solution certifiée par l'ANSSI

Stripe

Vous pouvez utiliser PayPlug.



Proofpoint

Vous pouvez utiliser Altospam.



Vous souhaitez prendre des notes ?

Vous souhaitez prendre des notes ?

GÉRER LA CRISE

1	Définir un incident	p.28
2	Les étapes clés	p.29
3	Les grandes étapes d'une situation de crise	p.30
4	Les autorités	p.31
5	Diriger la crise	p.32
6	Quelles sont les constantes d'une cybercrise ?	p.33

Définir un incident

« incident lié à la sécurité de l'information, un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information ».

Source : Norme ISO 27000 Articles 3.31.

Portez une importance aux signaux faibles, qui sont les activités anormales détectées (par exemple, un pic de connexion pendant le week-end), et qui peuvent induire un comportement suspect pouvant porter atteinte à la sécurité de l'entreprise.

Qui consulter ?

Vous pouvez recevoir une notice simple et claire du dispositif national d'assistance aux victimes pour comprendre et réagir efficacement aux cyberattaques.
Cette ressource peut faciliter votre prise de décision en matière de cybersécurité !



SCANNEZ – MOI !



Retrouvez plus d'informations sur le site de l'[ANSSI](#) et [cybermalveillance.gouv.fr](#)

2 Les étapes clés



Les grandes étapes d'une situation de crise

1 Compréhension de l'attaque

Il faut renforcer le SI pour éviter les attaques futures, la confiance de reprise en main du système passe par sa compréhension et le contrôle de la menace.

3 types d'actions pour comprendre et s'améliorer :

1

Le live forensics (outil, moyen, canaux de contrôle, commande d'infiltration, exfiltration), pour mieux comprendre l'attaque.

2

Le post-mortem, la situation après-crise où l'analyse Inforensique va permettre d'identifier et mieux comprendre les événements.

3

L'audit (la cartographie et l'audit sont là pour donner une vision exhaustive du scope et des vulnérabilités persistantes) en vue d'une démarche d'amélioration continue du SI.

Toutes les mesures identifiées de remédiations ou de corrections de vulnérabilités devront être classées dans un plan et priorisées :

Mesures déployables immédiatement,

Mesures à déployer pendant la crise (isolation, nettoyage, renforcement),

Mesures à déployer post-gestion de crise (renforcement des systèmes de sécurité et maintenance de l'attaquant en dehors du SI).

1 Qui alerter ?

Vous devez, dès suspicion de cyberattaque contacter **immédiatement** la police/gendarmerie au 17.



En résumé :



Appelez le 17



Déclarez la violation de données personnelles à la **CNIL** dans les 72 heures



Visitez le **Campus Cyber**

2 Quelles démarches réaliser ?

En France, il est obligatoire de notifier la **CNIL** dès la détection de l'impact sur les données personnelles. Si ces données constituent un risque élevé pour les personnes concernées, il faut les en informer.

Il est nécessaire de documenter aux autorités la nature de la violation en renseignant le Quoi, Qui, Quand, Où, Comment. Si possible :

- Indiquer les catégories et le nombre approximatif d'enregistrements de données personnelles concernées et de personnes touchées par la violation
- Décrire les conséquences probables de la violation de données
- Spécifier les mesures déjà prises ou envisagées pour prévenir la récurrence de cet incident ou atténuer d'éventuelles conséquences négatives
- Désigner le responsable de la gestion de crise (n°téléphone et nom)



PRIORISER

Monopoliser les ressources adéquates et donner la priorité sur ce dossier



FAIRE FONCTIONNER

Ne pas avoir peur du fonctionnement en dehors des processus habituels (papiers et stylos)



ARBITRER

Arbitrer les impacts sur le business, sur les clients et le processus (ex: couper la connexion internet pendant X jours, impact clients/fournisseurs)



PORTER

Communiquer intérieurement sur la sécurité dans l'entreprise

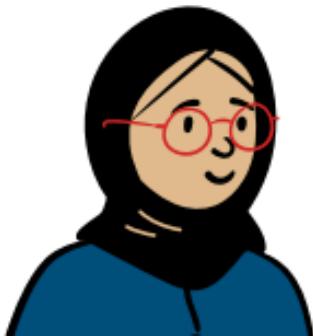


JOURNALISER

Journaliser les opérations de remédiation

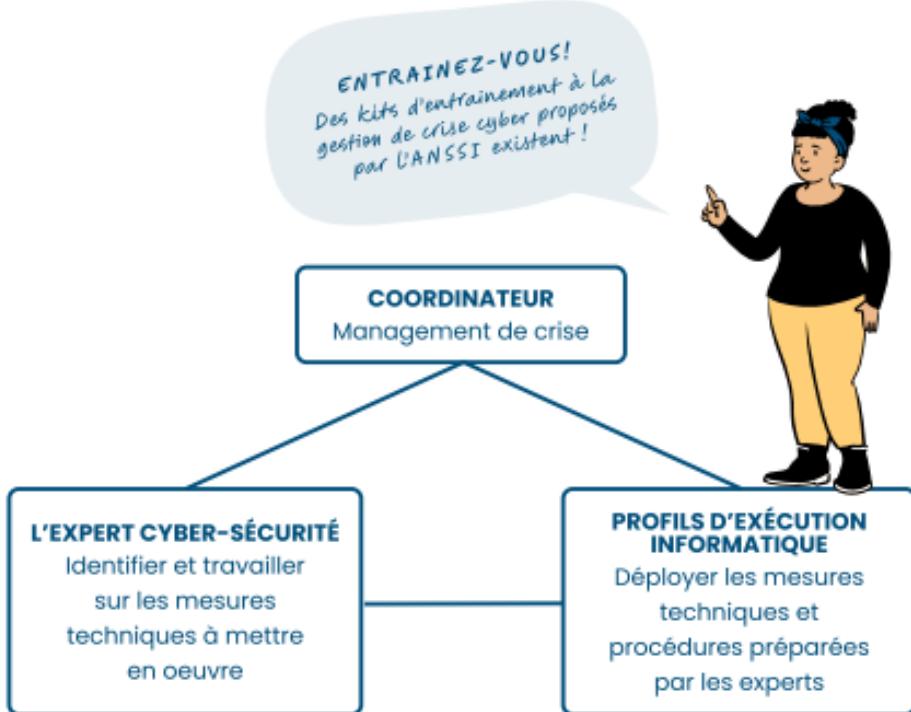
IMPORTANT

Vous devez conserver toute trace d'activités, décisions, observations et éléments de décision lors de la crise. Management, audit interne, actionnaires, clients, partenaires, presse et même autorités pourront être amenées à vous poser beaucoup de questions. Après la fin du traitement des impacts, il y a cet « après-crise » qui n'est pas à sous-estimer



Quelles sont les constantes d'une cybercrise ?

Lors d'une attaque, les notions de **35 heures, jours ouvrés, vacances et RTT**, n'ont plus vraiment de sens. Faites-vous aider sur cet aspect et **anticipez** ce point. Ces étapes nécessitent des compétences variées, classable en 3 points.



Une des constantes lors d'une cybercrise, c'est le besoin de faire appel, en un temps très court, pour une période potentiellement longue, à un volume important de ressources humaines pour participer aux différentes étapes de résolution d'une crise.

Restez vigilants quant à l'épuisement physique des collaborateurs, la fatigue humaine et psychologique est courante. Envisagez des options de restauration, de logements, de transports, ainsi qu'une aide psychologique.

Vous souhaitez prendre des notes ?

SORTIR DE CRISE

1

Organisation de sortie de crise

p.36

2

Retour d'expérience

p.37

Une fois la crise surmontée, il est important de définir et organiser un plan de sortie de crise.

Voici quelques recommandations :

Recommandations opérationnelles

- **Évaluer les solutions mises en place** pour savoir s'il faut les pérenniser
- **Mettre à jour** le registre de suivi de la crise
- **Réduire le rythme** de mobilisation des équipes pour éviter l'épuisement
- **Maintenir une surveillance** des systèmes d'information
- **Opérer une veille** sur internet (Darknet)

Recommandations stratégiques

- Faire un **plan d'action** pour récapituler les étapes clés dans le cas d'une nouvelle attaque : **PCA** (Plan de Continuité d'Activité) ou **PDA** (Personal Digital Assistant). Guide PCA : se référer au Glossaire.
- **Informier l'ensemble des équipes** de la sortie de crise : communiqué interne par exemple
- **Effectuer un bilan** des ressources humaines, pour les ajustements nécessaires (indemnisations, périodes de repos ...)

Le retour d'expérience

ÉTAPE 1 : A chaud

- organisé sous forme d'entretiens
- d'ateliers de collecte d'informations

ÉTAPE 2 : A froid

- présenter une synthèse des observations
- des recommandations
- le plan d'action associé

Voici quelques thèmes à aborder :

Et surtout, n'oubliez pas de parler de : la gestion de crise, la communication, la capacité technique et opérationnelle, la prise de décision et le suivi des actions

Pensez aussi à discuter des interactions internes et externes de l'entreprise, communiquez !



Vous souhaitez prendre des notes ?

GLOSSAIRE

A

ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information)

Agence gouvernementale française chargée de la sécurité informatique et de la protection des systèmes d'information (SI).

Attaquant

Personne ou groupe qui tente de pénétrer ou d'exploiter un système informatique de manière malveillante.

Attaque de force brute

Tentative d'accès à un système en testant toutes les combinaisons possibles de mots de passe ou de clés. C'est un passage en force.

Attaque de l'homme du milieu (Man in the middle)

Interception des communications entre deux parties sans leur consentement.

Attaque par pulvérisation de mots de passe

Méthode utilisant un mot de passe courant pour tenter d'accéder à plusieurs comptes.

Authentification forte avec multifacteurs

Processus de vérification de l'identité d'un utilisateur en utilisant plusieurs méthodes indépendantes.

B

Blacklistage

Action de bloquer l'accès à un système ou réseau à certaines adresses IP ou utilisateurs identifiés comme malveillants.

C

CNIL (Commission Nationale de l'Informatique et des Libertés)

Autorité administrative française indépendante chargée de veiller à ce que les données informatiques et libertés individuelles soient respectées.

Site internet : cnil.fr

C

Confidentialité

Préservation de la restriction d'accès à l'information aux seules personnes autorisées.

Conformité Réglementaire

Respect des lois et normes en vigueur concernant la protection des données.

Chiffrage

Processus de conversion des données en un format codé pour empêcher l'accès non autorisé.

Cyberattaque

Attaque informatique visant à endommager, perturber ou accéder illégalement à des systèmes informatiques, et plus généralement au système d'information.

Cybercrise

Situation d'urgence et dégradée résultant d'une attaque ou d'une menace significative contre les systèmes informatiques ou les réseaux.

Cybersécurité

Ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un État, d'une entreprise, etc.

D

Digital Operational Resilience Act (DORA)

Règlement européen qui est une déclinaison sectorielle de la directive NIS pour le secteur financier. Proposition de règlement introduite en septembre 2020 par la Commission Européenne.

Référence : Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022.

Disponibilité

Capacité d'un système à être opérationnel et accessible lorsque nécessaire.

La disponibilité fait partie des critères SSI (disponibilité, intégrité, confidentialité, traçabilité).

D

DoS/DDoS (Denial of Service/Distributed Denial of Service)

Attaque visant à rendre une ressource informatique indisponible.

E

Expert en cybersécurité

Spécialiste en sécurité informatique chargé de protéger les systèmes contre les attaques numériques.

F

Firewall (Pare-feu)

Système de sécurité réseau qui surveille et contrôle le trafic entrant et sortant selon des règles prédéfinies.

Forensics

Pratiques et techniques utilisées pour recueillir, préserver et analyser des données informatiques dans le cadre d'une enquête.

G

Guérilla

Méthode de lutte asymétrique, souvent utilisée pour décrire des conflits dans le cyberspace.

I

Incident de sécurité

Événement indésirable et potentiellement dommageable en matière de sécurité informatique.

Infiltration/d'exploitation

Processus par lequel un attaquant accède et utilise un système informatique à des fins malveillantes.

Intégrité

Assurance que les informations sont authentiques et n'ont pas été altérées.

L'intégrité fait partie des critères SSI (disponibilité, intégrité, confidentialité, traçabilité).

Injection de SQL

Type d'attaque exploitant des failles de sécurité dans les applications utilisant des bases de données SQL.

L

LPM (Loi des Programmations Militaires)

Loi française encadrant notamment les aspects de la sécurité nationale, y compris dans le cyberspace.

Référence : LOI n° 2023-703 du 1er août 2023.

M

Malware

Logiciel malveillant conçu pour endommager ou exploiter des systèmes informatiques.

Management de crise

Processus de gestion des événements majeurs ou des crises, y compris dans le domaine de la cybersécurité.

Menaces actuelles

Dangers actuels dans le domaine de la cybersécurité, comme les malwares ou les attaques par ransomware.

N

NIS2 (directive SR12)

L'objectif principal de la Réglementation NIS2 est d'améliorer la résilience des infrastructures et des services numériques face aux cybermenaces en constante évolution.

N

Notification des incidents

Obligation légale de rapporter les violations de sécurité ou incidents affectant les données personnelles ou la sécurité d'un réseau. Elle concerne tous les responsables de traitement de données à caractère personnel.

O

OIV (Opérateur d'Importance Vitale)

Entités identifiées par l'État comme cruciales pour le fonctionnement de la nation.

OSE (Opérateur des Services Essentiels)

Opérateur tributaire des réseaux ou systèmes d'information, qui fournit un service essentiel dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

OODA (Observe, Orient, Decide, and Act)

Processus décisionnel pour répondre efficacement aux incidents.

P

Pare-feu (Firewall)

Système de sécurité réseau qui surveille et contrôle le trafic entrant et sortant selon des règles prédéfinies.

Phishing

Technique de fraude en ligne visant à obtenir des informations sensibles (identifiants, mots de passe, etc.) en se faisant passer pour une entité de confiance.

Post-mortem

Analyse réalisée après un incident pour comprendre ce qui s'est passé et améliorer les mesures de sécurité.

Prévention

Mesures et actions visant à éviter ou réduire les risques de cyberattaques ou de pertes de données.

P

PCA (Plan de Continuité d'Activité)

Ensemble des mesures identifiées au sein d'une organisation permettant d'anticiper les conséquences de l'apparition d'une crise sur son activité principale.
Voir : https://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf

PDA (Personal Digital Assistant ou Assistant numérique personnel)

Petit terminal portable combinant les fonctionnalités d'un ordinateur et d'un smartphone. Il permet d'automatiser les processus et de gagner du temps dans l'exécution des tâches d'une entreprise.

PDCA (Plan Do Check Act)

Processus décisionnel pour améliorer son SSI.

Profils d'exécution informatiques

Professionnels chargés de mettre en œuvre les mesures techniques et procédures définies par les experts en cybersécurité.

PSSI (Politique de Sécurité du Système d'Information)

La PSSI reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration...) en matière de sécurité des systèmes d'information (ssi).

R

Ransomware

Le ransomware est une menace de sécurité qui cible les données et systèmes. C'est un malware qui empêche l'accès aux fichiers ou à certaines fonctionnalités (ou toutes) systèmes. Pour récupérer l'accès, une rançon est demandée.

S

Sécurité DNS

Mesures pour protéger le système de noms de domaine contre les cyberattaques.

Security Information and Event Management (SIEM)

Solution permettant de collecter, analyser et interpréter les données de sécurité des systèmes informatiques.

SI (Système d'Information)

Ensemble organisé de ressources (matériel, logiciel, personnel, données, procédures) permettant d'acquérir, traiter, stocker et diffuser de l'information.

SSI (Sécurité des Systèmes d'Informations)

Moyens techniques, organisationnels, juridiques et humains déployés pour empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information.

Spearphishing

Cette méthode de piratage ciblée consiste à usurper l'identité d'un de vos contacts pour vous piéger.

Spoofing

Usurpation d'identité électronique (téléphone) pour masquer la véritable identité de l'attaquant

Spyware et Keyloggers

Logiciels espions enregistrant les frappes au clavier pour obtenir des informations confidentielles.

T

Tactique de harcèlement

Stratégies utilisées pour entraver, déranger ou contrer les actions de l'attaquant.

V

Virus

Logiciel malveillant qui se duplique et se propage à d'autres ordinateurs.

VPN (Virtual Private Network)

Réseau privé virtuel offrant une connexion sécurisée et cryptée sur Internet.

Vishing

Variante du phishing utilisant la communication vocale (par exemple, les appels téléphoniques) pour obtenir des informations sensibles.



FICHES PRATIQUES

Fiche pratique

Boîte à outils de gestion de crise en cas de cyberattaque

1 Avant-crise



Exercices réflexes

Réaliser plusieurs mises en situation afin de mieux anticiper une future attaque en repérant les points les plus sensibles et constituer une **démarche réflexe**



Constituer une équipe type

S'entourer de personnes compétentes et formées



Former le personnel

Sensibiliser sur des bonnes pratiques et des gestes à adopter afin d'éviter une quelconque erreur humaine



Sauvegardes régulières des contenus sensibles

2 Pendant



Appeler le 17



Application des exercices réflexes

Mettre en exécution les instructions préparées au préalable par les experts



Protéger la confidentialité



Sécuriser l'environnement et le personnel



Garder une communication interne et externe

3 Après-crise



Remédiation



RETEX et debriefing

Vous souhaitez prendre des notes ?

Fiche pratique

Créer un mot de passe robuste

Les 4 points clés !



Unique



Secret



Robuste



À renouveler

1

Prendre un film que vous adorez

* Exemple : Batman – The Dark Night

3

Renforcer le tout en tapant la date du film sans appuyer sur la touche MAJ

* Exemple : éà&& (caractères associés aux chiffres)

2

Prendre les premières lettres des mots et y ajouter une majuscule

* Exemple : Btdk

4

Renforcer le tout avec la date de sortie du film,

* Exemple : 2011

5

Le mot de passe est prêt !

* Exemple : Btdkéà&&2011

Vous souhaitez prendre des notes ?

Fiche pratique

Comment éviter l'effet domino ?



L'entreprise possède un patrimoine (actif, humain)



Le patrimoine est :
exposé à des
menaces
porte des
vulnérabilités



Il faut 205 jours pour qu'une entreprise découvre qu'elle a été cyberattaquée



Ces vulnérabilités favorisent la réalisation des menaces, avec une certaine probabilité



La mise en place de mesures de protection permet de réduire l'impact des menaces



4 options de gestion du risque s'offrent à vous:

- **Tolérer** : être conscient du risque et l'accepter
- **Traiter** : agir afin de diminuer le nombre de sinistres ou l'importance de leurs impacts
- **Terminer** : arrêter le processus ou les actifs qui créent ce risque
- **Transférer** : contracter une cyberassurance pour prévenir le risque

Ces attaques ont évolué pour devenir plus agiles, plus furtives et plus complexes à identifier



Vous souhaitez prendre des notes ?

Les règles de base de l'ANSSI

1

- Choisir avec soin ses mots de passe

2

- Mettre à jour régulièrement ses logiciels

3

- Bien connaître ses utilisateurs et ses prestataires

4

- Effectuer des sauvegardes régulières

5

- Sécuriser l'accès Wi-Fi de son entreprise

6

- Être aussi prudent avec son smartphone ou sa tablette qu'avec son ordinateur

7

- Être prudent lors de l'utilisation de sa messagerie

8

- Protéger ses données lors de ses déplacements

9

- Télécharger ses programmes sur les sites officiels des éditeurs

10

- Être vigilant lors d'un paiement sur Internet

11

- Séparer ses usages personnels des usages professionnels

12

- Prendre soin de ses informations personnelles, professionnelles et de son identité numérique



Vous souhaitez prendre des notes ?

BIBLIOGRAPHIE

- Accueil Réseau certa. (s. d.).
<https://www.reseaucerta.org/>
- Certification des hébergeurs de données de santé. (s. d.). Agence du Numérique en Santé.
<https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de donnees-de-sante>
- Dispositif d'assistance aux victimes d'actes de cybermalveillance. (s. d.). CYBERMALVEILLANCE.GOUV.FR.
<https://www.cybermalveillance.gouv.fr/bonnes-pratiques>
- Entreprises et commerces. (s. d.). Accueil - Gendarmerie nationale.
<https://www.gendarmerie.interieur.gouv.fr/conseils/entreprises-et-commerces>
- Guide des bonnes pratiques de l'informatique | ANSSI. (s. d.). Agence nationale de la sécurité des systèmes d'information.
<https://cyber.gouv.fr/publications/guide-des-bonnes-pratiques-de-linformatique>
- Hiscox Assurances. (2022). Rapport Hiscox 2022 sur la gestion des cyber-risques.
<https://www.hiscox.fr/courtage/sites/courtage/files/documents/rappport-gestion-cyber-risques-2022.pdf>
- N°1 de la sécurité du cloud et la cybersécurité des endpoints | Trend Micro. (s. d.). Trend Micro.
https://www.trendmicro.com/fr_fr/business.html
- Phishing initiative. (s. d.).
<https://phishing-initiative.eu/contrib/>
- Rapport 2023 sur le coût d'une violation de données. (2024).
<https://www.ibm.com/fr-fr/reports/data-breach>
- Risques cyber : Des pistes pour la protection des entreprises. (2022, 7 septembre).
<https://www.economie.gouv.fr/risques-cyber-pistes-protection-entreprises>

- Saisir la CNIL. (s. d.).
<https://www.cnil.fr/fr/agir/saisir-la-cnil>
- (s. d.). Agence nationale de la sécurité des systèmes d'information.
<https://cyber.gouv.fr/>
- <https://www.internet-signalement.gouv.fr/PharosSI/>
- SecNumCloud pour les fournisseurs de services Cloud | ANSSI. (s. d.). Agence nationale de la sécurité des systèmes d'information.
<https://cyber.gouv.fr/secnumcloud-pour-les-fournisseurs-de-services-cloud>
- Sécuriser son organisation | ANSSI. (s. d.). Agence nationale de la sécurité des systèmes d'information.
<https://cyber.gouv.fr/securiser-son-organisation>
- Sécurité du réseau. (s. d.). Cisco.
<https://www.cisco.com/site/fr/fr/products/security/network-security/index.html>
- Signaler un spam. (s. d.).
<https://www.signal-spam.fr/>
- Direction Générale des Entreprises & CGPME. (2015, juillet). Guide PCA en cas de crise majeure. [entreprises.gouv.fr](https://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf).
https://www.entreprises.gouv.fr/files/files/directions_services/politique-et-enjeux/entrepreneuriat/Guide-PCA-en-cas-de-crise-majeure.pdf
- Baker McKenzie | Solutions for a Connected World. (s. d.). Baker McKenzie.
<https://www.bakermckenzie.com/en/>
- La cybersécurité des entreprises – Prévenir et guérir : Quels remèdes contre les cyber virus ? - Sénat. (s. d.-b). Sénat.
<https://www.senat.fr/rap/r20-678/r20-6780.html>



Coralie ALEXANDRU - Goufrane BENAZZA - Mollys CURTAT - Lamia ZIACHI - Nino BERBER -
Loïc LEFORESTIER - Thai-Son TRAN QUANG - Tristan REBEYROL - Natacha TWYFFELS -
Matthieu MARCHAND - Hugo MENSAH - Chloé FAYE

mm
BORDEAUX