RÉDIGÉ À PARTIR DES RECOMMANDATIONS DE L'ANSSI

# CYBERSÉCURITÉ

## Guide opérationnel à l'usage des Entreprises de Taille Intermédiaire

Édition 2021-2022


**CLUB ETI ILE-DE-FRANCE**

Commission Transformation Digitale

# SOMMAIRE



# ÉDITORIAL

*Par **Alain Conrard***
*Directeur général du groupe Prodware*
*Parrain de la Commission Transformation Digitale du Club ETI Ile-de-France*

**Toutes les entreprises sont uniques, avec des marchés différents, des savoir-faire spécifiques, des histoires singulières et des intérêts propres. Pourtant, toutes les entreprises ont aujourd'hui quelque chose en commun : toutes sont exposées au risque cyber.**

En effet, la menace cyber et ses conséquences délétères sont désormais présentes dans la vie quotidienne de nos entreprises. Ces trois dernières années, la révolution numérique et la crise Covid ont considérablement transformé nos entreprises et ouvert de nouvelles brèches, par de nouveaux usages et de nouvelles technologies.

Ces changements sont de véritables relais de croissance pour une cybercriminalité internationale, professionnelle et organisée. Il faut avoir conscience que **la cybercriminalité est aussi une industrie**, certes d'un type spécial qu'on pourrait qualifier de parasitaire. Mais c'est **une industrie à part entière qui croit en même temps que les autres**.

**Cette menace concerne particulièrement les ETI. Celle-ci sont devenues des cibles de choix.**

Tout d'abord parce qu'elles sont fortement créatrices de valeur, cette valeur que les cybercriminels veulent s'approprier. En effet, **les ETI sont les poumons de notre économie** qui génèrent à elles seules 1000 milliards d'euros de chiffre d'affaires et représentent 25% de l'emploi en France.

Ensuite parce que **les ETI sont à la fois puissantes et fragiles**. Ainsi, elles sont des cibles idéales car elles possèdent des dynamiques de croissance plus fortes que de nombreux grands groupes. Elles n'ont pas pour autant l'hygiène cyber et les moyens de ces derniers. Par ailleurs, 75% des ETI sont projetées, et donc exposées, à l'international. En France, elles sont souvent ancrées dans des territoires éloignés des grandes agglomérations et des grands centres de secours.

Alors que 50% des ETI ont été attaquées entre 2020 et 2021, et que toutes subiront de nouvelles tentatives d'intrusion, il est donc temps de prendre la juste mesure de ce risque macroéconomique, et surtout de prendre individuellement et collectivement les mesures de protection qui s'imposent. **Il en va ni plus ni moins que de la survie de nombreuses entreprises.**

**Dans ce contexte de cyberguerre, le METI* et les ETI du Club se sont organisées depuis plus d'un an.**

Ce vademecum est une restitution fidèle des **échanges de pair à pair** et des **interventions d'experts** qui ont eu lieu tout au long de l'année 2021-2022, au sein de ce Club riche de la diversité de ses entreprises.

# ÉDITORIAL

Nous y abordons de façon méthodique, solidaire et transparente les dimensions incontournables de la cybersécurité de nos ETI, au regard des moyens humains et financiers propres à cette catégorie d'entreprise.

**Cette boîte à outils structure et synthétise le travail collectif de nos ETI en quatre grands volets :**

- **Comprendre l'état de la menace**
- **Structurer la gouvernance cyber de son entreprise**
- **Préparer son ETI et se prémunir contre les risques**
- **Traverser toutes les étapes crise de l'attaque à la remédiation**

Bien entendu, ce document sera évolutif à l'image de la menace qu'il affronte. Cette première édition a été réalisée par et pour les ETI, afin qu'aucune d'entre elles ne se sente désarmée ou isolée dans la préparation de cet axe stratégique d'entreprise.

**À la dynamique de croissance des ETI, il faut désormais intégrer une dynamique de protection contre la cybercriminalité.** Car la première est désormais en partie dépendante de la seconde. Il est aujourd'hui vital de savoir résister à la cybermenace. Puisse ce vademecum être une inspiration dans ce sens pour le plus grand nombre d'entre nous. ●

***Alain Conrard***

* Mouvement des Entreprises de Taille Intermédiaire

# INTRODUCTION

# INTRODUCTION

## Les enjeux autour du risque cyber : tous concernés

L'informatique est devenu un facteur d'efficacité et de compétitivité : si la transformation numérique est désormais indispensable, les dommages des pertes de données et d'exploitation deviennent inacceptables pour les organisations.

Chacune dispose d'un système d'information **plus moderne, plus distribué mais aussi plus exposé** : toute organisation, dès lors qu'elle est connectée, devient vulnérable aux cybercriminels. Avec l'**exposition croissante aux outils digitaux** (Internet, IoT…) et l'**augmentation du recours au télétravail**, le risque cyber prend une ampleur inédite.

Contrairement au risque de panne technique, connu et relativement maîtrisable, **le risque cyber est changeant, polymorphe, et complexe à gérer** – notamment pour des ETI qui ne disposeraient pas d'une gouvernance ou de compétences cyber définies.

## Les ETI : une cible privilégiée

**Le risque cyber pèse particulièrement sur les ETI**. Poumon de l'économie française, elles représentent **¼ des emplois français**, **1 000 milliards d'euros de chiffre d'affaires**, et sont très ouvertes à l'international avec **35% des importations françaises** à leur actif. Pourtant, elles sont encore peu structurées et protégées face à la menace cyber. Elles sont, de fait, une **cible idéale pour les attaquants** – en tant que telles, ou comme porte d'entrée vers les grands groupes ou les pouvoirs publics dont elles soit souvent fournisseurs.

## Un constat : la maturité des ETI progresse… mais des freins subsistent

L'ensemble des dirigeants semble avoir pris conscience de la **nécessité de s'armer face au risque cyber**. Selon le **Baromètre Digital des ETI 2021** *(Enquête EY – APAX avec le soutien du METI et de Gilles Babinet – Conseil National du Numérique)*, la cybersécurité constitue la priorité des dirigeants dans le domaine numérique, et **le seul domaine numérique dans lequel les ETI prévoient d'augmenter leurs budgets d'investissement**.

## Face au risque cyber, la mobilisation se concrétise

La prise de conscience est réelle : **les ETI doivent désormais se donner les moyens humains et financiers de mettre en place une protection efficace et structurée**. Face à l'ampleur du risque, il est urgent de convaincre les dirigeants d'engager ces transformations.

**Le Club ETI Ile-de-France se mobilise pour accompagner ce mouvement**, à travers une programmation dédiée et des échanges réguliers de pair à pair, notamment via sa commission Transformation Digitale. Ce guide, destiné à l'ensemble des ETI et PME du Club, rassemble les expériences, expertises et bonnes pratiques partagées lors de la mobilisation cybersécurité de décembre 2021 et à travers le cycle cybersécurité de la Commission.

# L'ESSENTIEL :
# Trois jalons-clés pour préparer l'entreprise à repousser les attaques et en réduire les impacts

## S'organiser : volet gouvernance, volet technique

- Le risque majeur doit être compris par le dirigeant, qui doit **l'élever au niveau stratégique adéquat** et l'infuser dans toutes les couches de l'écosystème.
- Il faut penser l'entreprise non comme une forteresse, mais comme **partie prenante d'un écosystème interconnecté** : la sécurité numérique doit infuser toutes les parties prenantes. Cela peut passer par de la sensibilisation et / ou de la contractualisation.
- Le risque cyber doit être pensé comme **multidisciplinaire et non technique**.

## Constituer une bonne hygiène de base

- Le **Guide d'hygiène informatique** de l'ANSSI détaille 42 règles de base en la matière. Le guide **13 règles d'hygiène de base pour les TPE/PME** est également à consulter.
- La **charte informatique** définit les règles d'utilisation des outils numériques par les collaborateurs de l'entreprise. La **PSSI** constitue les fondations de sa sécurité numérique.
- L'hygiène de base et la mise en conformité réglementaire (ex : RGPD) sont primordiales. Une fois le socle réglementaire constitué, l'**analyse des risques** doit être conduite.

## Se préparer à la crise

- **Objectif :** ne pas passer par l'étape de sidération qui empêche la réaction rapide.
- **Anticiper l'absence de moyens** de communication et **l'inaccessibilité** de tous les serveurs de l'entreprise (exemple : prévoir tableaux blancs et feutres pour travailler).
- Prévoir la **répartition des rôles** (exemple : savoir qui prend la décision de couper l'accès à Internet).
- Prévoir un **plan de gestion de crise**, un **plan de continuité d'activité** et un **plan de reprise d'activité**.
- Constituer une **politique de sauvegardes déconnectées et testées**.
- Communiquer, en interne et en externe.
- **Sensibiliser** tous les acteurs et collaborateurs : le facteur humain est clé.
- **S'entraîner** régulièrement.

# INTERLOCUTEURS-CLÉS
# À contacter en cas d'attaque

**Les contacts téléphoniques de ces interlocuteurs doivent impérativement être à jour et conservés en-dehors du SI.**

## Interlocuteurs immédiats pour la gestion de crise et la remédiation

- Les **CSIRT privés et régionaux** pour obtenir une aide de premier niveau
- **Cybermalveillance.gouv.fr** pour signaler l'incident
- Vos **prestataires cyber** pour initier la remédiation

## Interlocuteurs des secteurs stratégiques

- L'**ANSSI** pour les administrations et les opérateurs régulés
- La **DGSI** pour les entreprises présentant un intérêt spécifique en matière d'économie, de recherche, de protection de l'État français

## Judiciarisation et enquête

- En fonction de la zone dont dépend l'entreprise : la **Police Nationale (OCLCTIC)** ou la **Gendarmerie Nationale (COMCyberGEND)** pour ouvrir l'enquête, réunir les preuves et identifier l'attaquant
- La **CNIL** pour signaler une brèche dans le respect du RGPD

# AVERTISSEMENT ET RECOMMANDATION

## Paiement des rançons et couverture assurantielle

En juin 2022, un groupe de travail consacré au développement de la couverture assurantielle du risque cyber a été mis en place par le Gouvernement. À l'issue de ces travaux, la Direction Générale du Trésor publie le rapport « Le développement de l'assurance du risque cyber », qui détaille un plan d'actions décliné en 4 axes.

**On peut notamment y lire que l'indemnisation du paiement des rançons par les assureurs sera autorisée, sous condition d'un dépôt de plainte :**

*« Conditionner l'assurabilité du paiement des rançons au dépôt de plainte par la victime permettrait de préserver la viabilité d'entreprises contraintes de s'acquitter de la rançon en dernier recours sans mettre en péril la répression de la cybercriminalité. Le remboursement de la rançon par l'assureur serait subordonné au dépôt de plainte par la victime sous 48 heures. Alors que de nombreuses victimes renoncent à déposer plainte afin de préserver leur image, une telle mesure permettrait de faciliter les investigations en informant systématiquement les autorités judiciaires et en permettant de mieux connaître les méthodes des cybercriminels. »*

### *Deux positions antagonistes*

- Le **paiement des rançons par les assureurs a souvent été dénoncé comme une incitation au crime**, en encourageant la récidive et entretenant ainsi le cercle vicieux des attaques (position tenue par Guillaume Poupard, Directeur général de l'Agence Nationale de la Sécurité des Systèmes d'Information, en 2021).
- La Direction du Trésor **tempère le risque que les entreprises françaises deviennent des cibles privilégiées**, en soulignant qu'aucun état de l'OCDE n'interdit le paiement des rançons.

### Trois raisons de ne pas payer une rançon et de ne pas accepter les propositions d'assurance associées

1. Depuis la publication de cette nouvelle politique et la possibilité de payer une rançon, **les Advanced Persistent Threats augmentent**. Les entreprises françaises deviennent une cible de choix pour les attaquants cyber qui demandent des rançons.
2. **Le paiement d'une rançon est considéré par les États-Unis comme une opération de financement du terrorisme.** Dans le cadre du *Cloud Act*, les États-Unis peuvent attaquer en extraterritorialité une entreprise étrangère ayant payé une rançon cyber. La publicité sur ce paiement expose donc les entreprises françaises à des attaques américaines.
3. **Le paiement ne garantit en aucun cas le déblocage du système.** Dans la plupart des organisations criminelles, ce sont des filiales différentes qui développent le code, diffusent le code, et négocient les rançons.

# CHAPITRE 1

## Comprendre l'état de la menace

# Étendue de la menace

## Chiffres-clés

**1/2** 1 ETI sur 2 a fait l'objet d'une cyberattaque entre 2020 et 2021 (source : Enquête METI Covid-19 – Suivi de l'impact sur les ETI #21, 16 avril 2021)

**100%** Toutes les ETI subiront de nouvelles tentatives d'intrusion

**3e** En 2021, les dommages de la cybercriminalité équivalent à la 3e économie mondiale (source : Cybercrime magazine)

**24%** L'Europe représente 24% des cyberattaques (source : IBM)

## Un constat : toutes les entreprises sont concernées

- Toute entreprise est concernée par la menace cyber, dès lors qu'elle est **exposée à Internet**.
- Les **administrations** et le **secteur industriel** constituent une cible privilégiée.
- **Les ETI sont particulièrement visées**, en tant que sous-traitants et partie intégrante de la chaîne de valeur des grands groupes et des organisations stratégiques.
- **Mettre à niveau son plan de cybersécurité est indispensable** pour protéger sa propre entreprise et ne pas constituer une faille dans la chaîne de valeur de ses partenaires.

## ZOOM | Typologie de la menace : quatre grands types de risques cyber sont recensés par le gouvernement

### *Cybercriminalité*

- Des attaques peuvent cibler les **particuliers** mais aussi les **entreprises** et les **administrations**.
- Elles visent à obtenir des **informations personnelles** afin de les exploiter ou de les revendre (données bancaires, identifiants à des sites marchands, etc.).
- **Hameçonnage** (« phishing ») et « **rançongiciel** » sont des exemples connus d'actes malveillants portant préjudice aux internautes. Pour s'en prémunir, des réflexes simples existent.

### *Espionnage*

- Très **ciblées et sophistiquées**, les attaques utilisées pour l'espionnage à des **fins économiques ou scientifiques** sont souvent le fait de groupes structurés.
- Elles peuvent avoir de lourdes conséquences pour les **intérêts nationaux**.
- De fait, il faut parfois **des années** à une organisation pour s'apercevoir qu'elle a été victime d'espionnage, l'objectif de l'attaquant étant de **maintenir discrètement son accès** le plus longtemps possible afin de **capter l'information stratégique** en temps voulu.

### *Sabotage*

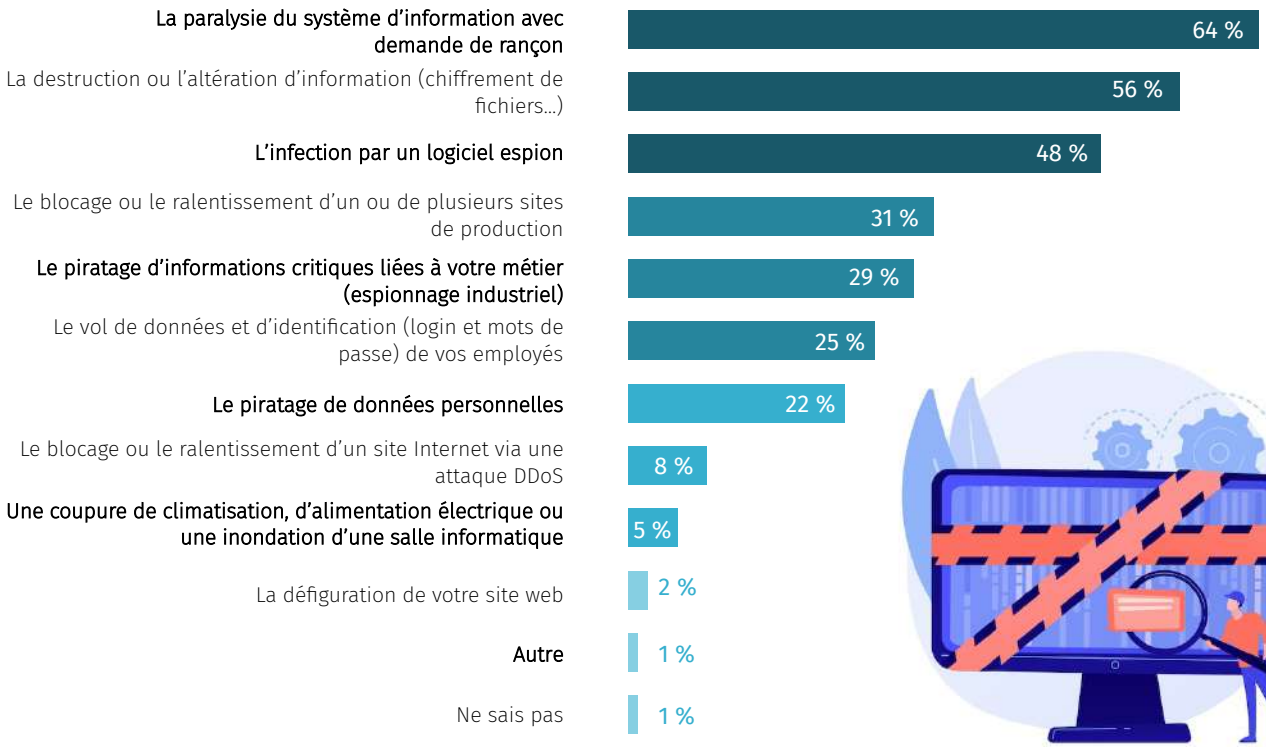
- Le sabotage informatique est le fait de **rendre inopérant** tout ou partie d'un système d'information d'une organisation **via une attaque informatique**.
- Il s'apparente à une « **panne organisée** », frappant tout ou partie des systèmes, selon le type d'atteinte recherchée.

### *Atteinte à l'image*

- Ces opérations sont lancées à des fins de **déstabilisation** contre des administrations et des entreprises et régulièrement relayées par les réseaux sociaux.
- Elles sont **fréquentes et généralement peu sophistiquées**, faisant appel à des outils et des services disponibles en ligne.
- De l'exfiltration de données personnelles à l'exploitation de vulnérabilité, elles **portent atteinte à l'image de la victime** en remplaçant le contenu par des revendications politiques, religieuses, etc.

## Les principales craintes des ETI en matière cyber

***« Parmi les risques suivants, lesquels redoutez-vous le plus ? »***




*Source : Sondage réalisé par Orange Business Services, L'Usine Nouvelle et B2B Intelligence, 2018*

# Comprendre les principaux types d'attaques

## Chiffres-clés

**25%** Les attaques par rançongiciel ont augmenté de 25% entre 2019 et 2020 (Source : ANSSI)

**93%** des entreprises sont victimes de tentatives de fraudes (Source : Euler Hermes)

**1/4** des faits de cybercriminalité recensés par la Gendarmerie concerne des escroqueries (arnaque au président, fraude au virement, etc.) (Source : COMCyberGEND)

## Trois grands types d'attaques coexistent

1. **Les attaques diffuses :** sans cible précise, elles **visent un public large** (virus, phishing, ransomware) et sont **facilement contournables** par des procédures de sécurité classiques.
2. **Les attaques opportunistes :** d'un **niveau technique plus avancé**, elles visent les **organismes les moins sécurisés** dans un objectif de gain immédiat (vol de données personnelles…). De fait, les cybercriminels **changeront rapidement de cible** en cas de difficulté à réussir l'attaque.
3. **Les attaques ciblées :** elles visent des informations ou des systèmes sensibles dans une **organisation clairement identifiée**. Les criminels visent une **cible précise**, avec un objectif clair (voler des données confidentielles…). Ces attaques sont longuement préparées et présentent un niveau technique élevé.

*Source: Wavestone*

## ZOOM | L'attaque au rançongiciel
***Source : ANSSI***

Un **rançongiciel** – ransomware en anglais – est un programme malveillant dont le but est d'**obtenir de la victime le paiement d'une rançon**. Les rançongiciels figurent au catalogue des outils auxquels ont recours les cybercriminels motivés par l'appât du gain.

**Lors d'une attaque par rançongiciel**, l'attaquant met l'ordinateur ou le système d'information de la victime **hors d'état de fonctionner de manière réversible**.

➡ *En pratique, la plupart des rançongiciels chiffrent par des mécanismes cryptographiques les données de l'ordinateur ou du système, rendant leur consultation ou leur utilisation impossibles. L'attaquant adresse alors un message non chiffré à la victime où il lui propose, contre le paiement d'une rançon, de lui fournir le moyen de déchiffrer ses données.*

### *Tendances*

La majorité des attaques par rançongiciels sont opportunistes et **profitent du faible niveau de maturité cyber de leurs victimes**. Il arrive parfois qu'un attaquant associe au rançongiciel un ou plusieurs autres **programmes malveillants** (crypto mineurs, cheval de Troie, etc.).
Il devient dès lors possible d'utiliser de manière illégale les **ressources matérielles** des équipements compromis ou de **s'emparer des données** présentes sur le système d'information.

De récentes attaques par rançongiciels ont mis en évidence le **danger d'un impact systémique sur un secteur d'activité** qui, en ciblant des entreprises sous-traitantes ou clés du secteur, pourrait amener à le déstabiliser. Le préjudice va alors bien au-delà de la perte des données ou du paiement d'une rançon puisque **les organisations victimes doivent faire face à de nombreuses autres conséquences** : arrêt de la production, chute du chiffre d'affaires, risques juridiques (par exemple liés au RGPD dans le cas où des données personnelles ne sont plus accessibles), altération de la réputation, perte de confiance des clients, etc.

Ces attaques génèrent souvent une **rupture ou une dégradation d'activité chez la victime**. Dans le cas d'une entreprise, il peut en aller de sa survie. **Le rançongiciel est une menace sérieuse aux conséquences potentiellement durables pour les organisations.**

**Il est essentiel de rappeler que le paiement des rançons entretient cette activité criminelle et ne garantit pas à la victime la récupération de ses données** **(lire p. 9)**

*Source : Guide « Attaque par rançongiciels, tous concernés : Comment anticiper et réagir en cas d'incident ? », ANSSI*

**Note :** outre l'absence de garantie de récupération des données, le paiement d'une rançon peut être considéré par certains États (États-Unis notamment) comme une opération de financement du terrorisme. Les entreprises entretenant des activités avec ces États qui paieraient une rançon pourraient donc se voir condamnées de manière extraterritoriale.

## L'œil de l'expert : l'arnaque au Président et la fraude au virement

*Par Stéphane Gillot, Directeur Régional Ile-de-France, Référence DSI*

### *L'arnaque au Président*

**Mode opératoire de l'arnaque au Président**

- Un escroc se faisant passer pour le Président d'une entreprise **prétexte un motif urgent** pour obtenir un **virement de fonds** vers un compte basé à l'étranger.

**La préparation**

- Les fraudeurs **regroupent des informations** sur l'entreprise visée, ses dirigeants, ses process, via des sources publiques et par la ruse

**La prise de contact**

- Les fraudeurs utilisent des **technologies légales** (achat de numéro de téléphone, d'adresse mail…) pour contacter l'entreprise sans éveiller les soupçons des salariés.

**La pression psychologique**

- L'escroc **contacte un salarié et le dupe**. Les filiales sont des cibles privilégiées, tout comme les périodes suivant un rachat d'entreprise (management encore en période d'installation). L'escroc **prétexte une situation d'urgence** et réclame toute confidentialité afin d'obtenir le virement des fonds.

**Une fois les fonds virés, ils transitent par plusieurs pays pour en complexifier la traçabilité.**

**Si la fraude n'est pas décelée immédiatement, il n'est plus possible d'alerter la banque pour figer les fonds.**

## L'œil de l'expert : l'arnaque au Président et la fraude au virement

*Par Stéphane Gillot, Directeur Régional Ile-de-France, Référence DSI*

### *La fraude au virement*

**Mode opératoire de la fraude au virement (IBAN)**

- L'escroc adresse un mail à la société victime, se faisant passer pour un fournisseur et réclamant le paiement de factures en **indiquant de nouvelles coordonnées bancaires**.
- Les **attaques sont ciblées**, pour rendre la relance crédible aux yeux de la victime.
- Les fonds virés transitent également par plusieurs pays.
- La fraude au virement peut également consister à **modifier les comptes bancaires** fournisseurs lors d'une intrusion dans le SI, ou à **intercepter des factures fournisseurs** et à en modifier les coordonnées bancaires.

### *Face à ces arnaques, les dispositifs de sécurité traditionnels restent peu efficaces*

- Les arnaques sont **ciblées** et les escrocs généralement **bien renseignés** sur l'actualité et les pratiques de l'entreprise.
- Le contact avec l'entreprise est généralement effectué par mail, **non bloqué par les antispams** car utilisant une nouvelle adresse à chaque tentative, et non envoyé en nombre.
- La transmission des coordonnées bancaires frauduleuses se fait via une pièce jointe qui ne contient aucune menace et n'est donc **pas détectée par les antivirus**.

**La réponse à ces menaces est donc avant tout organisationnelle : elle relève de la formalisation des processus de virement et de la formation des collaborateurs.**

- Pour la prévention des collaborateurs, voir chapitre III : Préparer son ETI et se prémunir contre les attaques.
- Solutions opérationnelles de sécurisation des virements : Mata IO, Trustpair, SIS ID, Ibansecure.

## D'autres types d'attaques

### *Le phishing*

- Le cybercriminel se fait passer pour un **tiers de confiance** (banque, administration, fournisseur d'accès…) et diffuse un message frauduleux à une large liste de contacts.
- Le message invite les destinataires à **mettre à jour leurs informations personnelles** (souvent bancaires) sur un site falsifié vers lequel ils sont redirigés.
- Les données saisies sont **récupérées** par les escrocs.
  - **Le smishing :** phishing reposant sur l'envoi de SMS frauduleux.
  - **Le vishing :** arnaque par voie téléphonique, reposant sur l'utilisation de technologies vocales

### *La défiguration*

- Elle consiste **modifier l'apparence ou le contenu** d'un site, et donc à altérer l'intégrité des pages.
- Le cybercriminel **exploite souvent des vulnérabilités connues** (défaut de sécurité), mais non corrigées du site. L'atteinte réussie du site peut prendre différentes formes : ajout d'informations sur une page ou remplacement intégral d'une page.

**RESSOURCE COMPLÉMENTAIRE**

**Pour suivre les campagnes de cyberattaques ayant cours**
Suivi des menaces et incidents – ANSSI : https://www.cert.ssi.gouv.fr/cti/

# CHAPITRE 2

## Structurer la gouvernance cyber de son entreprise

# Organiser la gouvernance cyber

## Chiffres-clés

**26 mois**

En moyenne, les RSSI (responsables de la sécurité des systèmes d'information) restent en poste **26 mois** au sein d'une organisation.
*Source : Nominet CISO Stress Report, 2020*

## MÉTHODOLOGIE
### Comment structurer sa gouvernance cyber ?

### *Le risque cyber est stratégique*

À ce titre, il doit être **élevé au même niveau que les autres risques** (juridique, financier…).
Une **stratégie de sécurité numérique** doit être élaborée :

- **Désigner un référent dédié à la mission** (RSSI, responsable sécurité…) rattaché à la direction et disposant d'un budget propre
- **Élaborer une charte informatique** pour définir l'usage des outils numériques par les collaborateurs ; signé par chacun d'entre eux, elle leur sera opposable.
- **Rédiger une Politique de Sécurité du Système d'Information** (PSSI) : plan d'action définies pour maintenir le niveau de sécurité au sein de l'organisation, elle doit être régulièrement réévaluée.

### *La gouvernance de la cybersécurité s'inscrit dans une démarche GRC*

- **Gouvernance :** définir une politique de cybersécurité, organiser et piloter la sécurité, définir les moyens et responsabilités inhérentes.
- **Risques :** identifier les menaces et le degré d'exposition de l'organisation ; analyser la sensibilité de ses actifs et données.
- **Conformité :** mesurer le respect des exigences légales et réglementaires ; garantir la confiance des parties prenantes.

### *Les enjeux de cybersécurité pour les ETI*

- **Définir la stratégie et l'organisation de la sécurité**
  - Organiser la fonction sécurité et la gouvernance cyber
  - Rédiger une PSSI et un socle documentaire de la Sécurité de Systèmes d'Information (SSI)
  - Construire une feuille de route SSI à 3 ans
- **Identifier, analyser et traiter les risques**
  - Réaliser une analyse de risque globale du périmètre entreprise
  - Intégrer la question de la sécurité à chacun des projets

**Viser et évaluer la conformité**

- Définir un cycle pour la mise en conformité à la PSSI
- Définir un socle de sécurité réaliste (guide d'hygiène de l'ANSSI, ISO 27002, NIST…)

**Assurer la continuité et la résilience**

- Construire un plan de continuité d'activité à trois composantes : utilisateurs, informations, gestion de crise
- Tester et proposer des exercices d'entraînement

## L'essentiel : rédiger une PSSI

*Source : Agence Nationale de Sécurité des Systèmes d'Information (ANSSI)*

- **La PSSI est le document de référence de l'organisation en matière de SSI.** Elle définit les objectifs de cybersécurité de l'entreprise et les moyens associés ; elle témoigne de la vision stratégique de la direction de l'organisme en matière de SSSI.
- La PSSI doit être **rédigée au niveau global de l'organisation**, et peut être déclinée en PSSI techniques par métiers.
- Elle doit être **diffusée à l'ensemble des parties prenantes** interagissant avec le SI (utilisateurs, sous-traitants, prestataires…).
- Elle doit **évoluer** pour prendre en compte les évolutions de l'organisation et de son contexte.

***L'ANSSI recommande une démarche d'élaboration en 4 phases :***

1. **Organisation** du projet PSSI et constitution du référentiel
2. **Recueil** des éléments stratégiques
3. **Choix** des principes et déclinaison en règles adaptées au contexte
4. **Finalisation** et **validation** de la PSSI et de son plan d'action

- Au préalable, une **analyse des risques** facilite l'élaboration de la PSSI
- L'élaboration de la PSSI gagne à être **organisée sous la forme d'un véritable projet** : chef de projet désigné, groupes de travail, ressources dédiées, calendrier et livrables identifiés (notes de cadrage et de stratégie, synthèse des règles et des impacts, PSSI, plan d'action).


PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Guide pour l'élaboration d'une politique de sécurité de système d'information

PSSI

SECTION 2
MÉTHODOLOGIE

**Pour aller plus loin**

**Guide d'élaboration de politiques de sécurité des systèmes d'information**
**Par l'ANSSI**

Bien que rédigé en 2004, ce guide conserve sa pertinence.

Une fiche méthode et une synthèse sont également disponibles.

## ZOOM | La fonction de RSSI (Responsable de la Sécurité des Systèmes d'Information)

### *Missions*

- **Définir**, **piloter**, **mesurer** et **améliorer** le niveau de sécurité dans l'organisation.
- **Accompagner**, **conseiller** et **sensibiliser** les équipes
- Prendre en charge les **sujets opérationnels** de la sécurité

### *Profil*

- **Expert sécurité expérimenté**, culture générale technique, en capacité de dialoguer avec les interlocuteurs IT, métiers et direction

### *Positionnement*

- Au sein d'une **direction des risques** ou rattaché à un **organe central** (ex : direction générale), idéalement indépendant de la DSI

### *Arbitrage à opérer au sein de chaque organisation*

- Embaucher un expert en **interne** ou **externaliser** la compétence.

### *Une solution : le RSSI à temps partagé*

- Expert en cybersécurité, il prend en charge les tâches associées au rôle de RSSI
- Généralement mobilisé au sein de l'entreprise **1 à 3 jours par semaine**
- Pour des missions de **6 à 18 mois**
- **Cas d'application** : RSSI en transition ou en recrutement ; PME ou ETI ne pouvant embaucher un ETP ; compétences insuffisantes en interne sans souhait de recrutement

**Retrouvez en annexe (p. 47) le détail de la fiche de poste du RSSI, conçue par l'ANSSI**

**Pour aller plus loin**

Panorama des métiers de la cybersécurité
Par l'ANSSI

### Bonnes pratiques et observations

- **La direction générale** doit impulser une vision stratégique et être motrice sur le sujet de la gouvernance cyber.
- **Instaurer des comités de sécurité** est utile pour suivre les KPIs propres à la sécurité et apprécier l'évolution des risques.
- Les ETI du Club privilégient les **RSSI à temps partagé** et externalisés.

### Pièges à éviter

- **Attendre l'arrivée d'une crise cyber** pour organiser sa gouvernance : une fois que la crise survient, il est déjà trop tard.
- **Négliger les livrables** (PSSI, plans formalisés) et ne pas garantir leur accessibilité en toute circonstance, en cas de blocage du SI notamment.

## Les écueils rencontrés par les ETI dans la mise en place de leur gouvernance cyber

**Un manque de temps** pour organiser la gouvernance cyber, et **un manque de moyens financiers** à affecter aux projets cyber.

La **sensibilisation de la direction générale** est capitale pour assurer son rôle moteur et libérer les ressources temporelles et financières en la matière.

**Des difficultés de rémunération** et d'**identification** des profils experts : le marché de l'emploi est en forte tension sur ces métiers.

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

- **Débloquer des budgets à consacrer à la cybersécurité**. L'ANSSI recommande d'y consacrer 5 à 10% du budget informatique.
- **Insister sur l'importance de la démarche top-down**, et de la vision stratégique portée par la direction, pour débloquer une politique cyber efficace.

**À sa DSI :**

- Se (re)positionner comme **garant de la sécurité** et agrégateur de solutions
- Présenter l'état de l'**attribution des compétences sécurité** au sein de l'ETI
- Lancer la **conception de la PSSI et de la charte informatique**

**RESSOURCES COMPLÉMENTAIRES**

La cybersécurité pour les TPE/PME en douze questions, ANSSI

Guide des bonnes pratiques de l'informatique, ANSSI

## ILLUSTRATION : Structuration de la gouvernance cyber du groupe Leader suite à une attaque

*Témoignage de **Christophe Benoist**, DSI*

*Basé à Saint-Ouen-l'Aumône (95), le groupe Leader est spécialiste du travail temporaire et des prestations en ressources humaines.*

*L'entreprise réalise 665 millions d'euros de chiffre d'affaires (2021) et emploie 650 collaborateurs.*

### L'attaque

- En 2021, suite à une **opération de phishing** auprès des collaborateurs du groupe, les données de Leader sont **intégralement cryptées**.
- L'attaque intervient **au moment de la paye** de ses 13 000 intérimaires.
- Le système d'information est **intégralement bloqué** et plonge l'entreprise dans la sidération.
- L'entreprise constitue une **cellule technique** et un **comité de pilotage** de crise.

➡ Dès la résolution de la crise et la reprise de l'activité, deux jours après l'attaque, Leader a amorcé une **nouvelle stratégie de gouvernance cyber**.

### Recours à un RSSI externalisé

- Leader a pris la décision d'avoir recours à un **RSSI externe**. Ce dernier est rattaché à la direction générale, afin que la DSI ne soit pas « juge et partie » de la situation (Ch. Benoist)
- **Le rôle du RSSI :** assurer la sécurité cyber du groupe ; « faire office d'irritant, en testant régulièrement [l'entreprise] ».

### Recrutement d'un risk manager

- Un **risk manager** a été embauché et rattaché à la cellule d'amélioration continue, dont les compétences ont été élargies.
- **L'éducation à l'hygiène informatique** pour l'ensemble des salariés est devenue une priorité.

### Recommandations de Christophe Benoist

➡ **Sensibiliser autour de soi** (pairs, partenaires) pour assurer la sécurité de toute la chaîne.

➡ **Solliciter les organismes spécialisés**, type ANSSI, pour accompagner la structuration.

➡ **Définir un budget précis** lié à la cybersécurité.

Source : « Victime d'une cyberattaque, Groupe Leader se dote d'un risk manager et d'un RSSI », LesEchos.fr, 4 février 2022

# Mettre en place des audits de sécurité

## Chiffres-clés

**207** En moyenne, les organisations constatent leurs failles de sécurité après 207 jours

**2e** La menace interne pointe au 2e rang des risques IT en Europe pour l'année 2020

*Source : IBM*

## Quelle est la finalité d'une démarche d'audit ?

Il s'agit d'une procédure régulière qui a pour but d'**évaluer le niveau de sécurité d'un système d'information** sous l'angle de l'organisation, des processus et de l'outillage. Il permet d'énumérer et de prioriser les actions correctives, et d'établir ou d'affiner la PSSI.

Ainsi, un audit de sécurité a pour finalité de garantir la disponibilité du système, de protéger l'intégrité des données et la confidentialité des accès. (Source : Cyber jobs)

L'**audit de compromission** permet d'identifier la présence d'un acteur malveillant dans le système, tandis que l'**audit de sécurité** ne teste pas si le système est déjà infecté, mais évalue son niveau global de sécurité.

### L'essentiel : panorama des enjeux de l'audit cyber

*Source : Prodware*

- Les cybercriminels exploitent les **failles de vulnérabilité externes et internes**. L'audit cyber doit permettre de **démontrer la résilience de l'organisation** face à ces menaces.
- Les **audits méthodologiques et de conformité** évaluent les process et les outils de l'organisation pour structurer sa PSSI.
- Le recours à des **hackers éthiques** permet de détecter des failles de sécurité pour que la DSI y remédie.
- Le **cyber scoring** permet d'analyser automatiquement les vulnérabilités de l'organisation et d'évaluer sa maturité technique.
- Le **plan de reprise d'activité (PRA)** est un ensemble de moyens techniques et de démarches, accompagné de tests permettant d'évaluer sa bonne fonctionnalité.
- Le **service de recherches des compromissions** permet d'identifier les compromissions passées ou présentes : un hacker peut en effet investir un SI et y demeurer longuement sans être détecté.

## L'œil de l'expert : l'audit de sécurité du SI

*Par Marc Lionti, Consultant cybersécurité senior, Inquest*

### *Objectifs d'un audit de sécurité*

- **Évaluer et renforcer le niveau de préparation** cyber de l'organisation : identifier les *quick wins* et les lacunes qui augmentent le risque, proposer un plan d'action priorisé
- Obtenir une **note technique d'assurabilité** (qualité du risque) lors d'une recherche d'assurance
- **Éprouver les défenses** mises en place sur le SI, dans une démarche d'amélioration permanente son engagement.

### *Méthodologie d'un audit de sécurité*

- Utiliser un **référentiel d'audit** permet de proposer une grille d'analyse objective et complète, et de garantir l'évaluation de l'ensemble des sujets cyber. *Exemple : norme ISO 27002.*
- L'audit est à déployer sur le **SI industriel**, le **SI bureautique et métiers**, les **data centers** et les **ressources cloud**.

### *Déroulement d'un audit de sécurité*

1. **Entretiens :** cadrage des audits avec les interlocuteurs désignés
2. **Documents :** collecte de données sur l'organisation et ses process
3. **Évaluation :** évaluation des aspects en fonction de la sécurité et de l'écart avec les bonnes pratiques
4. **Synthèse :** production d'une synthèse par domaine sous forme de fiches concrètes et priorisées
5. **Actions :** établissement d'un plan d'action à mettre en œuvre progressivement

## ZOOM | Le cyber rating (ou cyber scoring)

Le **cyber rating** est un ensemble de paramètres permettant d'**évaluer le niveau de maturité en cyber sécurité d'une organisation**. Ainsi, des agences de cyber rating attribuent désormais une « cyber-note » aux entreprises dans l'objectif de quantifier le risque cyber auquel elles sont exposées.

***Ces organisations collectent et analysent des informations accessibles publiquement :***

- Les vulnérabilités présentes sur les **sites web** de l'entreprise
- La réputation des **adresses IP publiques** de l'entreprise
- La protection des **adresses mail** de l'entreprise
- La présence de données de l'entreprise sur le **Dark Web**

***Le cyber rating :***

- Identifie les **vulnérabilités** de l'entreprise ;
- Expose leur **gravité** ;
- Propose des **recommandations** adaptées ;
- **Surveille** l'entreprise et alerte régulièrement de tout **changement**.

Sources : Menaya et Wavestone

### *Exemple : plan d'action global axé sur les principales faiblesses de l'entreprise*

- *Auditer et renforcer ses moyens de **sauvegarde** et de **restauration***
- ***Sensibiliser** ses utilisateurs et protéger sa messagerie*
- *Préparer des **kits documentaires** papier ou externalisés de gestion de crise*
- *Connaître son **niveau d'exposition interne***
- *Auditer et renforcer la sécurité des **comptes à privilèges***
- *Mettre en place une politique de gestion des **vulnérabilités internes***
- *Auditer l'ensemble des **infrastructures internes** pour identifier les faiblesses*
- *Mettre sous **surveillance en temps réel** l'activité de son SI pour gagner en visibilité*

### Bonnes pratiques opérationnelles

- Une **gouvernance bien structurée** et la **présence d'un RSSI** *(voir 2.A – Organiser sa gouvernance cyber)* permettent d'assurer la bonne conduite de l'audit.
- Les **résultats des tests d'intrusion et des audits** peuvent être le déclencheur d'une prise de conscience de la direction générale.
- Les **tests d'intrusion** exécutés par des hackers éthiques sont fréquents. L'**audit méthodologique** est plus rare et gagne à être étendu.
- **Multiplier les partenaires** pour réaliser des audits permet de bénéficier d'approches complémentaires.
- L'audit cyber doit cibler l'**infrastructure globale** comme les **applications métiers**.
- L'**audit de compromission** est réalisable après l'attaque pour en reconstituer le déroulement (utile dans le cadre de l'enquête judiciaire et de l'expertise de l'assurance)

### Exemples de partenaires et outils à mobiliser

- **Exemples de prestataires d'audit cyber :** EY, Inquest, IT Trust, SysDream
- **Les EDR (Endpoint Detection Response) :** Harfanglab, Tehtris
- **Pour réaliser des audits de compromission :** cybermalveillance.gouv.fr ; liste de prestataires PASSI approuvés par l'ANSSI

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

- Présenter les **résultats d'audit** et de **tests d'intrusion** pour déclencher une **prise de conscience**

**À sa DSI :**

- Benchmarker **différents prestataires** pour auditer l'entreprise
- Réaliser des **tests d'intrusion**

# CHAPITRE 3

## Préparer son ETI et se prémunir contre les attaques

# Prévention : former et sensibiliser ses collaborateurs

## Chiffres-clés

**N°1** « Sensibiliser et former » est la première recommandation des 42 mesures du Guide d'hygiène informatique de l'ANSSI

**90%** Des incidents de sécurité sont imputables à l'erreur humaine

**60%** Des cyberattaques ont pour origine une faille humaine

*Source : Kaspersky Security Awareness, « Le facteur humain est un enjeu majeur de la cybersécurité en entreprise »*

## ZOOM | L'ingénierie sociale

### Définition

L'**ingénierie sociale** est l'acte de manipuler les humains pour procurer des informations confidentielles ou effectuer des actions nuisibles. Vulnérables à la tromperie, à l'influence et à la désinformation, les humains sont une cible privilégiée pour les attaquants.

Les attaquants s'appuient sur l'ingénierie sociale qui constitue souvent **le moyen le plus rapide d'atteindre leurs objectifs**. Ils sont innovants et utiliseront de nouvelles méthodes pour tromper et manipuler les victimes non préparées. Les protections techniques, même les plus onéreuses, peuvent être facilement contournées.

- **Un attaquant n'a besoin de réussir qu'une seule fois pour compromettre sa cible ; sa cible doit, en revanche, réussir 100% du temps pour éviter les compromissions.**
- **Une formation efficace est le seul moyen d'armer ses collaborateurs contre la tromperie et la désinformation.**

## L'essentiel : la collaboration DSI / DRH au profit de la prévention cyber

**La sensibilisation à la cybersécurité relève autant du périmètre de la DSI que de celui de la DRH.**

Une coopération entre les deux directions est absolument indispensable pour mener une campagne de formation efficace, et protéger au mieux l'entreprise des risques cyber liés à des failles humaines.

## MÉTHODOLOGIE
### Comment mettre en œuvre une campagne de cyber sensibilisation ?

*Démarche proposée par l'ESN Prodware*

**Kickoff**
- Présentation des enjeux
- Association des équipes projet IT et RH
  Planning de la campagne
- Plan de communication
  Appui de la Direction

**Intégration technique**
- Configuration des plateformes de formation
- Paramétrage des serveurs
- Import des utilisateurs et des groupes

**Campagne de phishing** (1 semaine)
- Préparation de l'attaque fictive
- Évaluation des résultats

**Évaluation cyber** (2 semaines)
- Enquête d'évaluation du niveau cyber des utilisateurs
- Analyse des résultats par le groupe

**Campagne de formation cyber**
- Définition du plan de formation annuel, fondé sur le résultat de l'analyse

ACCOMPAGNEMENT

**Pilotage et amélioration de la maturité cyber**
- Ajustement des contenus, gamification
- Évaluation continue et enquête annuelle
- Campagnes de hameçonnage régulières
- Support des managers / sponsors

Ajustements en continu

**Le recours à une solution de sensibilisation externe est particulièrement adapté aux ETI.**

**La plupart des solutions de cybersensibilisation procurent des contenus mais aussi des KPIs :**

- Taux de participation
- Évaluation des connaissances post-formation
- Taux de clics sur mails malicieux

### *Les facteurs clés de succès d'une démarche de cybersensibilisation*

*Par Cyrille Duvivier, Responsable Infrastructure, Cloud et Cybersécurité, Prodware*

Risque utilisateur évalué via des enquêtes et des campagnes d'hameçonnage et ajustement continu du plan de formation

Contenus cybersécurité préconstruits, attractifs, gradués et régulièrement renouvelés


Privilégier une solution efficace : approche Cloud, KPI et simulations d'attaque embarquées, interface utilisateur responsive

Des équipes DSI et DRH mobilisées pour la mise en œuvre et l'amélioration continue de la démarche

**Un entraînement régulier aux exercices cyber garantit la résilience de l'organisation :**

- **Pour les utilisateurs :** tests phishing, vishing, smishing (voir p. 15)
- **Pour les équipes IT :** test de restauration, test d'intrusion, de PRI et de PRA
- **Direction :** comités de crise

Source : Prodware

## Bonnes pratiques : la coopération DSI / DRH en faveur de la prévention cyber

- **Impliquer les managers** dans le suivi des formations cyber de leurs équipes *(exemple : via le monitoring de KPIs, l'attribution de primes…)*
- **Contextualiser les supports de formation** en fonction des enjeux et spécificités de chaque département ou métier
- Sensibiliser avec le même niveau d'exigence les **parties prenantes externes** ayant accès au SI de l'entreprise
- Intégrer la sensibilisation cyber **dès l'arrivée dans l'entreprise**, à l'onboarding des collaborateurs – voire proposer de suivre la formation avant même l'arrivée dans l'entreprise
- **Gamifier la prévention cyber** (quizz…), développer une **communication ludique régulière**
- **Réactualiser régulièrement la formation** est pour intégrer les nouveaux enjeux cyber
- **Monitorer la complétion des programmes** par les collaborateurs, relancer ceux qui n'auraient par réalisé la formation dans son intégralité

**Appliquer un principe de tolérance zéro sur le suivi de la formation cyber par les collaborateurs : pour protéger l'entreprise, chacun doit être sensibilisé.**

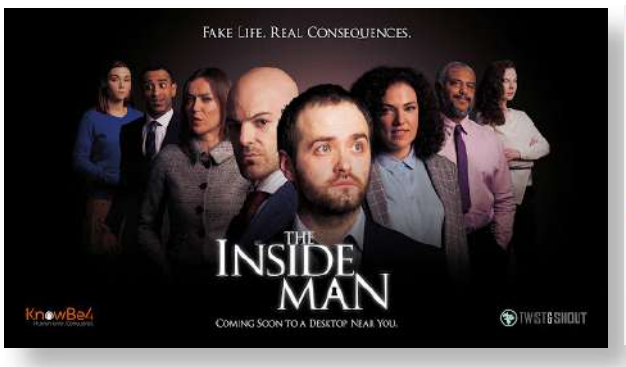
## ZOOM | La solution KnowBe4

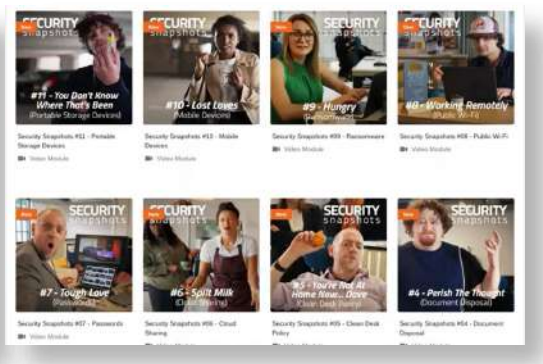
**Des contenus de sensibilisation courts et attractifs sont une clé de réussite des programmes de prévention cyber.**

La plateforme **KnowBe4** propose des programmes de formation à la cybersécurité, aux formats ludiques permettant de **susciter l'intérêt des collaborateurs** et d'assurer le bon suivi des formations.

**Parmi les contenus proposés :**

- Campagnes de sensibilisation et **tests de phishing** avec suivi de KPIs
- **Streaming de vidéos de sensibilisation** au format capsules ou mini-séries Netflix
- **Contenus multilingues** (adaptés aux entreprises disposant de filiales à l'étranger)
- Contenus **adaptables à chaque entreprise**




Gauche : *The Inside Man*, série originale KnowBe4, présente les concepts clés de la cybersécurité par le biais d'un contenu semblable à du divertissement

Droite : courtes capsules vidéos présentant de manière ludique et attractive les points clés de diverses thématiques cyber (mots de passe, wifi public…)

## ILLUSTRATION : Le plan de formation à la cybersécurité du groupe Prodware



*Témoignage de **Laurence Dubois**, DRH France ; **Cyrille Duvivier**, responsable Infrastructure, Cloud et cybersécurité ; et **Marc Lestienne**, DSI adjoint*

*Basé à Paris, le groupe Prodware est intégrateur de solutions numériques.*
*L'entreprise réalise 165,5 millions d'euros de chiffre d'affaires (2021) et emploie 1 065 collaborateurs.*

### La philosophie du groupe

- Au sein du groupe Prodware, **la transformation digitale dans son ensemble est considérée comme relevant à la fois du périmètre de la DSI et de celui de la DRH**. Le plan de prévention et sensibilisation contre le risque cyber est donc conçu conjointement entre les deux directions.

> *Dans la lutte contre la cybercriminalité, **la plus grande force des entreprises dépend désormais de leur maillon le plus faible : l'humain**. […] En tant qu'élément clé de leur politique de sécurité des Systèmes d'Information, les entreprises de toutes tailles ont donc besoin de **moyens permanents, systématiques et actualisés pour former et sensibiliser leurs collaborateurs aux enjeux liées à la cybersécurité**.*
>
> ***Mettre en place des campagnes de sensibilisation à la cybersécurité devient donc indispensable pour les entreprises** […]. Ces formations de sensibilisation à la cybersécurité doivent **soutenir les objectifs globaux de sécurité de l'entreprise en parvenant à modifier les comportements risqués des utilisateurs** tels que : cliquer sur un lien ou un fichier non vérifié, saisir des informations sensibles dans un formulaire de page web suspect ou communiquer des informations à une personne non vérifiée ou clairement identifiée comme étant un membre de l'entreprise.*

Source : Prodware

### Les solutions déployées

- Le groupe a conçu un plan de prévention ludique, reposant sur des solutions externalisées, des contenus attractifs et le suivi de KPIs précis.
  - **Utilisation de la plateforme KnowBe4** (vidéos de prévention au format mini-série)
  - **Envoi d'une newsletter thématisée**, graphique et amusante aux collaborateurs pour les informer de l'actualité des risques cyber
  - **Gamification** *(exemple : quizz de connaissances via Klaxoon ou AhaSlides)*
  - **Campagnes de tests de phishing** avec suivi de résultats globaux et individuels

### Les résultats obtenus

- **Quantitatifs**
  - Grâce aux campagnes de tests de phishing, le taux de clic inapproprié est passé de **28%** lors du premier test à **11%** après 2 mois
  - L'objectif est d'atteindre un taux de **0%**. Le suivi du programme de prévention est obligatoire : des relances régulières sont envoyées aux collaborateurs.
- **Qualitatifs**
  - Le programme de prévention a permis de créer une cohésion au sein de l'entreprise, et de développer un esprit de groupe entre les collaborateurs.

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

- Si ce n'est déjà fait, **organiser un échange entre DRH et DSI** autour de la prévention cyber, pour élaborer un plan d'action commun
- **Débloquer des ressources** (financières, humaines) pour la mise en place d'un plan de prévention à la cybersécurité

**À sa DSI :**

- **Mettre en place un plan de sensibilisation** concret pour l'ensemble des collaborateurs, en concertation avec la DRH
- Mettre en place des **exercices** de gestion de crise et des campagnes de test, avec suivi de KPIs

## RESSOURCES COMPLÉMENTAIRES


[Organiser un exercice de gestion de crise cyber]
**Guide pratique de l'ANSSI**


[Formation à la cybersécurité : MOOC SecNumacadémie.gouv.fr]
**Par l'ANSSI**

# Protection : sécuriser l'infrastructure et les applicatifs

## Qu'est-ce que la cyberprotection ?

La cyberprotection est l'**ensemble des moyens, techniques, humains ou juridiques**, qui contribuent à **assurer la cybersécurité d'une organisation**. La cyberprotection s'appuie notamment sur des mesures prises pour préserver la sécurité des systèmes d'information.

La sécurité technique est indissociable d'un **plan de formation soutenu et suivi**, à destination de l'ensemble des collaborateurs d'une organisation (tous niveaux hiérarchiques confondus), voire de ses parties prenantes externes.

## MÉTHODOLOGIE
### Comment organiser la sécurité de ses actifs ?

**La sécurité des actifs d'une organisation se décline en trois volets.**

### *Sécurité des utilisateurs et des terminaux*

- Les **antivirus**, **EPP** *(Endpoint Protection Plateform)* et **EDR** *(Endpoint Detection and Response)* permettent de lire et contenir la menace sur les postes et les serveurs.
- L'**authentification forte multi-facteurs** (MFA) et l'**approche « passwordless »** permettent de garantir l'identité des utilisateurs.
- Les **solutions de gestion des terminaux et d'apps** (**MDM**, *Mobility Device Management* ; **MAM**, *Mobile Application Management*) permettent de maintenir le niveau de sécurité des terminaux et des applicatifs de l'entreprise.
- Les **comptes à privilèges** doivent disposer de modalités d'accès renforcées au SI, via la mise en œuvre de « **bastions** ».

### *Sécurité périmétrique*

- Les **pare-feux** (Firewall et web application Firewall) permettent d'isoler les données et les actifs des risques extérieurs.
- Les **VPN** et le **chiffrement des flux** sécurisent les données en transit.
- Le **cloisonnement des réseaux** limite le risque ; le ***network access control*** doit permettre la connexion physique aux utilisateurs et terminaux autorisés uniquement.
- Les comptes à privilèges, **tiers et invités** doivent bénéficier d'un **accès contrôlé**, isolé du reste de l'entreprise.

### *Sécurité des données et des systèmes*

- Pour les sauvegardes, la **règle du 3-2-1-0 prévaut** : **3** versions d'une sauvegarde, sur **2** médias différents, **1** sauvegarde externalisée, et **0** erreur. L'**immuabilité** des sauvegardes doit être considérée.
- Les **données doivent être chiffrées** pour devenir inexploitables en cas de vol.
- La **détection des vulnérabilités** et l'**application régulière des correctifs** sur le SI est indispensable.
- Le **SIEM** *(Security Information and Event Management)* permet de collecter et de corréler les logs issus du SI, pour détecter des alertes de sécurité grâce à l'intelligence artificielle.
- Les **applications métiers** doivent également être soumises à une politique de cybersécurité stricte.

### L'œil de l'expert : le modèle « Zero trust »
*Par l'ANSSI*

Le principe du **Zero trust** consiste à **remettre en cause la confiance implicite** accordée aux demandes d'accès au système, qu'il s'agisse de demandes internes ou externes à l'organisation.
Le Zero trust n'est **pas une technologie en soi**, mais un **concept d'architecture**. Il consiste à mettre en place des **contrôles renforcés** de l'accès des utilisateurs au système d'information de l'entreprise.
**Attention : C'est une notion en cours de construction.**

***Pour réduire la confiance implicite, les contrôles doivent devenir réguliers, dynamiques et granulaires :***

- L'accès aux ressources doit être accordé **sur la base du besoin d'en connaître** ;
- L'accès doit être donné sur la base du **plus faible niveau de privilège nécessaire** pour réaliser la tâche ;
- Les demandes d'accès doivent être contrôlées de la même manière **quelles que soient leurs origines** (le périmètre « intérieur » ou « extérieur » de l'entité) ;
- La politique d'accès aux ressources doit être dynamique et prendre en compte un **large nombre d'attributs** (identités de l'accédant et de la ressource accédée, sensibilité des ressources sollicitées, analyse comportementale de l'utilisateur, horaires d'accès, etc.) ;
- L'entité doit veiller à la **sécurité de tous ses actifs** à l'occasion des demandes d'accès et de manière récurrente durant l'usage ;
- Les authentifications et autorisations d'accès aux ressources doivent faire l'objet de **réévaluations régulières**.

#### *Comment intégrer du Zero trust à un SI traditionnel ?*

Avant tout déploiement, **l'analyse de risque doit être à jour**. Plusieurs axes d'effort sont envisageables pour intégrer à un SI « traditionnel » les principes du Zero Trust :

- Une **gouvernance améliorée de l'identité** (politique stricte de mise à jour lors des départs, arrivées, mobilités).
- Un **cloisonnement des ressources plus granulaire et dynamique**. Cette « micro-segmentation » cloisonne les ressources en groupes qui ont une signification métier, et des accès associés aux données nécessaires.

- Une **utilisation des moyens d'authentification à l'état de l'art**
- Un **renforcement des moyens de détection** : les équipes de supervision de la sécurité (SOC) doivent être suffisamment formées, expérimentées et dimensionnées pour réagir aux alarmes de sécurité.
- Une **configuration à l'état de l'art de la sécurité des services**. Par exemple, pour le chiffrement de flux, TLS doit être configuré suivant le guide TLS de l'ANSSI.
- Une **conduite du changement** à mener auprès des utilisateurs (communication, sensibilisation). Le modèle Zero Trust est vu comme un levier de simplification de l'expérience utilisateur, il ne doit pas faire oublier que les utilisateurs sont les premiers concernés par la sécurité numérique de leur entité.

**La migration vers le Zero trust doit être progressive, pour aboutir à un modèle hybride.**

## Bonnes pratiques opérationnelles

- À nouveau, la **formation des collaborateurs est fondamentale**. Ils doivent constituer le **premier rempart** contre les attaques cyber. Les outils de protection, si pointus soient-ils, ne doivent en aucun cas susciter une confiance aveugle.
- Les accès des collaborateurs aux serveurs doivent être **régulièrement réévalués** ; il convient de supprimer les accès des comptes obsolètes *(ex : collaborateurs ayant quitté l'entreprise)*.
- Dans la gestion du **télétravail** et du **nomadisme**, veiller à mettre en place une authentification multi-facteurs, des VPN et des procédures de chiffrement des terminaux mobiles.
- Les **mots de passe** doivent être changés régulièrement et doivent pouvoir être modifié à la demande des utilisateurs (**SSPR** : *self-service password reset*).
- Les mêmes précautions doivent être appliquées aux **collaborateurs** et aux **prestataires extérieurs** à l'entreprise.
- Le niveau de protection doit être évalué **en continu** et **ponctuellement via des tests**. Faire appel à des sociétés spécialistes de l'audit (voir p. 22) permet d'évaluer son niveau.
- Les **données doivent être classifiées** ; une politique de **protection différenciée** en fonction de leur niveau stratégique doit être appliquée.
- L'ouverture des droits dans les applications métiers doit être **limitée au strict minimum** nécessaire pour un collaborateur.
- Attention aux données stratégiques fournies aux ressources IT et aux tiers dans le cas des **environnements Dev/Test**.

## ZOOM | Les bonnes pratiques des sauvegardes

- La **règle du 3-2-1-0** doit être appliquée (cf. *supra*)
- Les sauvegardes doivent être **isolées et régulièrement testées**
- Les **sauvegardes Cloud** doivent faire l'objet d'une attention particulière : elles ne constituent pas une sécurité absolue, car **leur durée de rétention est limitée**. Des sauvegardes complémentaires doivent être mises en place.
- Avec l'utilisation du Cloud, la sécurité des terminaux **reste sous la responsabilité de l'entreprise** : si celle-ci est corrompue, la sauvegarde Cloud sera inutilisable.

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

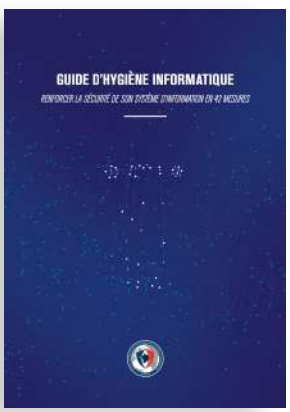
- Nul besoin d'accorder aux dirigeants des **comptes à privilèges** !
- Les appareils de la direction générale sont-ils **suffisamment sécurisés** (MFA, flux cryptés…) ?
- Le dirigeant applique-t-il les **recommandations précitées** ?

**À sa DSI :**

- Les principales **mesures de protection évoquées** (authentification multi-facteurs, EDR, chiffrement des flux, classification des données…) sont-elles appliquées au SI, aux collaborateurs, aux externes ?
- Le principe du **Zero Trust** est-il étudié et graduellement appliqué ?
- Les sauvegardes **répondent-elles aux best practices** ? Ont-elles été récemment **testées** ?

## RESSOURCES COMPLÉMENTAIRES

**Guides pratiques de l'ANSSI**




Guide d'hygiène informatique


Guide des bonnes pratiques de l'informatique


Charte d'utilisation des moyens informatiques et des moyens numériques

# S'assurer

## Chiffres-clés

**9%** **1%** Seules 9% des ETI et moins de 1% des PME ont souscrit une assurance cyber

**600** milliards **85** millions En France en 2020, le volume des primes d'assurance IARD est de 600 milliards d'euros, contre 85 millions pour les primes liées au risque cyber

*Source : LUCY : LUmière sur la CYberassurance, AMRAE, juin 2022*

## Qu'est-ce que le risque cyber ?

Le **risque cyber** correspond à l'ensemble des risques liées à une **utilisation malveillante** des systèmes d'information et des technologies de l'information des particuliers, des administrations ou des entreprises.

### Trois risques différents en découlent :

- **Le risque de responsabilité civile :** préjudice subi par le tiers et les frais de défense
- **Le risque de dommages aux biens (DAB) et pertes financières :** dommages de l'assuré
- **La gestion de crise :** frais de recherche, de communication, de notification, de défense devant la CNIL, fraude, sanction CNIL, etc (indépendamment d'une mise en cause d'un tiers ou de dommages subis par l'assuré)

### L'œil de l'expert : les solutions assurantielles proposées par les assureurs

*Par Nicolas Hélénon, Gérant, NeoTech Assurances (groupe Diot-Siaci)*

#### *Responsabilité civile – Préjudice du tiers*

- Conséquences d'une **violation de la législation** sur la protection des **données personnelles**
- Conséquences d'une **atteinte à la confidentialité** des informations
- Conséquences d'une **atteinte à la propriété intellectuelle** ou d'une atteinte à la **vie privée** ou du **droit à l'image**
- Conséquences d'**agissement diffamatoire,** de **publicité mensongère** ou de **dénigrement**
- Conséquences d'une **atteinte du SI** ou des **données d'un tiers** via le SI de l'assuré
- Conséquences d'un **déni de service d'un tiers** suite à une attaque logique
- Conséquences d'une **transmission de virus** à des tiers

#### *Volet DAB – Pertes financières de l'assuré*

- Frais de **reconstitution des données** et frais de **restauration des sauvegardes** suite à une atteinte aux données et aux SI
- Frais de **recherche** et frais de **décontamination** suite à une atteinte aux données et aux SI
- Frais d'**exploitation** ou **perte d'emploi** suite à une atteinte aux données et aux SI
- **Pénalité contractuelle** ou **SLA** (accord de niveau de service) suite à une atteinte aux données ou aux SI
- Conséquences pécuniaires suite à un **déni de service**
- Frais de mise en œuvre du **PCA** (Plan de Continuité d'Activité)

### *Volet gestion de crise*

- Frais de **recherche** et de **qualification** de l'incident
- Frais de **représentation** *(exemple : défense)* suite à une convocation ou enquête de la CNIL
- Frais de **notification** suite à une **injonction de la CNIL**
- Frais de **notification** suite une **obligation contractuelle**
- Frais de **monitoring**
- Frais de **communication**
- Frais de consultant en **sécurité informatique**
- Frais de consultant en cas de **tentative d'extorsion**
- **Fraude**

## ZOOM | État des lieux du marché de l'assurance cyber

- Les **grandes entreprises** sont très sensibilisées au risque cyber : 84% sont couvertes
- **ETI et PME sont sous-équipées** : respectivement 9% et moins de 1% sont assurées
- Les **actes de vente sont complexes** et nécessitent de répondre à des questionnaires avancés : les petites structures n'ont pas nécessairement les moyens de les mener à bien
- Les clients **manquent souvent de maturité** en matière de sécurité et prévention, prérequis pourtant indispensable du côté des assureurs : il convient d'investir dans ces deux volets pour accroître la confiance de ces derniers.
- Les intermédiaires (courtiers en assurance) ne sont **pas assez formés** au risque cyber

**Le marché se rétracte depuis 2020 avec l'augmentation exponentielle des attaques cyber.**

**Le volume des primes ne permet plus de couvrir les sinistres, ce qui a des conséquences concrètes sur le marché de l'assurance :**

- Baisse des garanties
- Baisse des capacités de garanties
- Augmentation des franchises
- Augmentation des primes (doublement, *a minima*)
- Augmentation des niveaux d'exigence et d'éligibilité à l'assurance cyber

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

- Est-on **assuré contre le risque cyber** ? Dans le cas contraire, il est urgent d'**engager le dialogue**.

**À sa DSI :**

- Comment **améliorer la gouvernance** cyber, **quels moyens débloquer** pour augmenter la préparation de l'entreprise et être **mieux perçu par les assureurs** ?

# CHAPITRE 4

## De l'attaque à la remédiation : Gérer et résoudre la crise cyber

# Gestion de crise : que faire en cas d'attaque

## Que se passe-t-il en cas d'attaque ?

- L'organisation assiste à un **blocage complet de son système informatique** : aucun service ni application ne fonctionne, les sites de production sont arrêtés, les accès aux messageries et aux données sont bloqués.
- Dans le cas de l'espionnage, **aucune perturbation n'est visible** par les utilisateurs, mais les données sont diffusées chez l'attaquant.
- L'attaquant est souvent présent dans le système d'information **bien en amont de l'attaque.**

### Parole d'expert
*Commandement de la Gendarmerie dans le Cyberespace (COMCyberGEND)*

- Pour permettre une attaque cyber, trois éléments sont nécessaires : **un bien** (les données), **une faille informatique** et un **attaquant**.
- Pour faire cesser l'attaque : il faut **soustraire l'un de ces trois éléments**.

### L'œil de l'expert : la gestion de crise
*Par Anne Doré, Présidente, Adhel*

**La gestion de la crise cyber doit se diviser en deux cycles.**

***Le cycle nominal continu***

- Dans une **logique d'amélioration permanente**, il consiste à **protéger** l'entreprise, à **éviter** la crise cyber et à **déterminer** les modalités d'organisation de la gestion de crise.
- Les mesures d'anticipation, de détection, de prévention doivent permettre de **maintenir les conditions de sécurité** de l'entreprise.
- L'objectif est le **Maintien des Conditions d'Anticipation** (MCA) :
  - **Cartographier les risques** pour connaître les actifs à protéger en priorité
  - Connaître les **typologies** d'attaques et d'attaquants
  - Établir et tester les **sauvegardes**
  - **Anticiper les risques** liés à l'utilisation d'un nouvel outil.
- Des incidents peuvent se produire, sans qu'ils ne soient suffisamment graves pour déclencher la crise. Ils doivent être **traités et réinjectés** dans le cycle d'anticipation.

## *Le cycle de crise*

### Ouvrir la crise

- Des indicateurs doivent être **établis en amont** pour déterminer le **niveau de gravité** de la crise
- Le **plan de gestion de crise** définit une **organisation adéquate**, sa structure et ses procédures, décisionnelles comme opérationnelles

### Contenir l'attaque

- Selon les modalités décrites dans le plan de gestion de crise, l'entreprise ouvre sa **salle de crise**, déploie ses **moyens de communication** et de **traitement informatique** prédéfinis
- Les **outils de pilotage et coordination** exceptionnels, réfléchis en amont, sont déployés
- Il est impératif que les **fiches réflexes** pour les procédures soient accessibles hors du SI
- La **direction générale** doit être mobilisée pour prendre les décisions
- **Objectifs :** limiter le périmètre de l'attaque, protéger les données saines

### Remédier

- Avant de rouvrir le système, l'ensemble des applications et données corrompues **doit être examiné**
- **La sortie doit être préparée** : l'entreprise doit assurer la transition vers un mode de fonctionnement opérationnel, puis arriver progressivement à un fonctionnement normal

### Clore la crise

- La sortie de l'état de gestion de crise doit être officialisée
- La clôture de crise doit être décidée **de manière collégiale**, sur la base d'une **analyse de risques**
- Les ressources et moyens de crise doivent être **démobilisés** ; les parties prenantes doivent être **remerciées** de leur mobilisation

**L'objectif du cycle de crise est de revenir à un cycle nominal le plus rapidement possible.**

## Bonnes pratiques opérationnelles

- Mettre en place des **services d'accompagnement psychologiques**, essentiels pour contrer le stress auquel sont soumises les équipes lors d'une attaque
- Garder en mémoire qu'en cas de blocage du SI, **rien n'est accessible** :
  - Garder ses **contacts prioritaires** accessibles hors du SI
  - Conserver les **coordonnées des collaborateurs** en-dehors du SI
  - Conserver **au format papier** le plan de gestion de crise, dans un endroit accessible et connu de tous
  - Prévoir le **matériel nécessaire** en cas d'inaccessibilité totale du SI (papier, feutres…)

### Qui contacter en priorité en cas de crise ?

1. **La CNIL** pour signaler une brèche dans le respect du RGPD
2. **La Police ou la Gendarmerie** pour déposer plainte et obtenir une aide de premier niveau : **OCLCTIC** (Office Centrale de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication – Police), **COMCyberGEND** (Gendarmerie)
3. **L'assureur** pour ouvrir un dossier
4. **Les prestataires cyber** pour gérer la crise et rétablir l'activité de l'entreprise
5. **Cybermalveillance.gouv.fr** pour signaler l'incident
6. **La DGSI** (Direction Générale de la Sécurité Intérieure)
7. **Le CERT-FR** (Computer Emergency Response Team)

## ZOOM | Le CSIRT

- Un **CSIRT** est une **équipe de sécurité opérationnelle**, composée d'experts de différents domaines (malwares, tests d'intrusion, veille, analyse forensique…).
- Elle est chargée de **prévenir** et de **réagir** en cas d'incidents de sécurité informatique.
- C'est une équipe qui **centralise et sert de relais**, que ce soit en interne ou externe de l'entreprise : la **communication** est l'une de ces fonctions principales.

**CSIRT :** Computer Security Incident Response Team
**CERT :** Computer Emergency Response Team

➡ ***Ils permettent de réaliser la threat intelligence et de répondre à une crise cyber***

**SOC :** Security Operation Center

➡ ***Il traite essentiellement de la surveillance des alertes de sécurité***

### *Dans quel cas les contacter ?*

- **En phase d'anticipation :** se préparer aux incidents, obtenir un état des lieux et une analyse de la menace
- **En réaction à un incident :** lever les doutes de l'organisation, répondre à un incident cyber avéré

### *Les CSIRT régionaux, en partenariat avec l'ANSSI*

Les CSIRT régionaux apporteront une **réponse concrète et immédiate** aux ETI victimes de cyberattaques, partout sur le territoire national, de la déclaration d'incident à la remédiation :

- **Centralisation des demandes d'assistance** suite à des cyberattaques et **plan de sensibilisation** des collectivités et des entreprises ;
- **Traitement** des alertes, réaction et qualification
- Interface entre les **victimes** et les **prestataires locaux** appropriés.

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

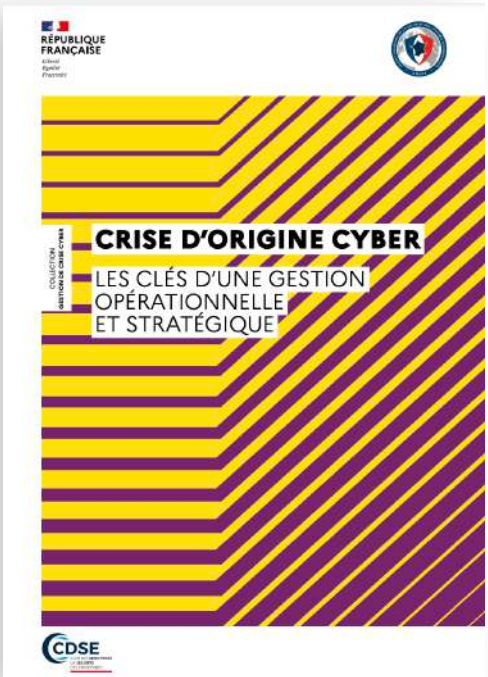
- Le **comité de gestion de crise** est-il établi ?
- En cas de crise, les **rôles** *(opérationnels, communication interne et externe, prise de contact avec les prestataires, l'assureur et les autorités)* sont-ils identifiés ?
- A-t-on défini les **critères de déclenchement** de la crise ?

**À sa DSI :**

- A-t-on un **PRA** et un **plan de gestion de crise** ? Sont-ils facilement localisables hors du SI ?
- Les **contacts** des autorités, prestataires et collaborateurs sont-ils disponibles hors du SI ?
- Les **fiches réflexes** sont-elles accessibles hors du SI ?

## Pour aller plus loin

**Guides pratiques de l'ANSSI**




Crise d'origine cyber : les clés d'une gestion opérationnelle et stratégique


Anticiper et gérer sa communication de crise cyber

# Remédiation : se reconstruire après la crise

## Qu'est-ce que la remédiation ?

La remédiation est **la phase qui suit l'identification d'un risque ou le traitement d'un incident**. Il s'agit de l'ensemble des actions apportées afin de **limiter l'impact du risque ou de l'incident**. Ces mesures sont consignées dans un plan de remédiation, ou définies de manière ad hoc par l'équipe de réponse à incident. (Source : Assises de la Cybersécurité)

### Analyse forensique

Elle consiste à **collecter et analyser les preuves d'une compromission**, et à déterminer avec précision le mode opératoire utilisé par l'attaquant et l'impact de l'attaque. Les preuves collectées et le rapport réalisé peuvent notamment être utilisés dans le cas d'un traitement juridique ou d'un dossier d'assurance.

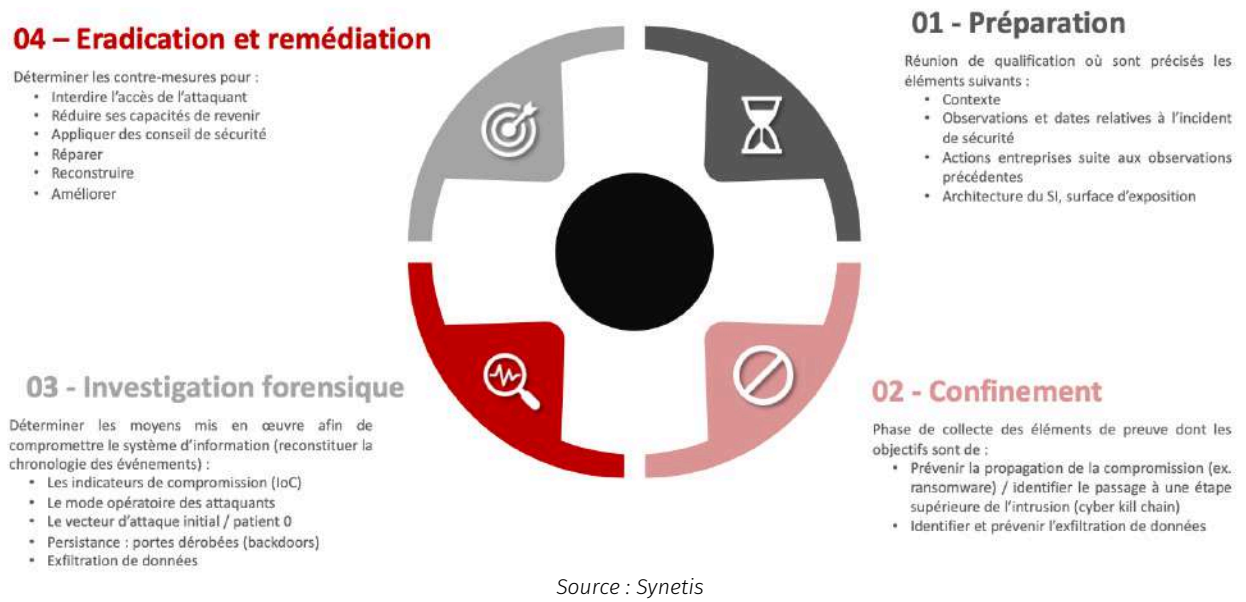
### Grey zone vers green zone

L'analyse forensique permet d'**identifier les plateformes impactées** (infrastructure possiblement corrompue : grey zone). La green zone est une infrastructure non corrompue reconstruite à l'état de l'art.

**L'œil de l'expert : la remédiation**

*Par Rémi Fournier, Directeur général, Synetis*

***Processus de réponse à un incident de sécurité***




*Source : Synetis*

## *Remédiation : les trois grands scénarios*

| Critères | Cas 1 – Impact majeur | Cas 2 – Impact important | Cas 3 – Impact faible |
|---|---|---|---|
| Niveau d'information sur les événements | Partiel (pas assez de logs) | | Complet |
| Annuaire(s) Active Directory | Compromission | | Partiellement compromis (serveurs / stations spécifiques) |
| Messagerie | Compromission | Pas de compromission | |
| Réseau | Compromission | Pas de compromission | |
| Sauvegarde | Compromission | | Pas de compromission |
| Sauvegarde | Sauvegarde locale et externalisée : hors service<br>Sauvegarde déconnectée | | Sauvegarde locale, externalisée et déconnectée : opérationnelle |
| Serveurs | 90% des machines chiffrées | 20% des serveurs | 5% des machines chiffrées |
| Stations de travail | 50% des machines chiffrées | 30% des machines chiffrées | 5% des machines chiffrées |
| Solution virtualisation | Compromission | Pas de compromission | |
| Rétablissement du service (dégradé / normal) | 1 mois / 6 mois | 2 semaines / 3 mois | 5 jours / 2 semaines |
| Perte de données | 1 semaine | 1 semaine | 1 journée |
| **Scénario retenu** | **Zone grise / zone verte** | **Zone grise / zone intermédiaire** | **Sécurisation zone grise** |

*Source : Synetis*

## MÉTHODOLOGIE
### Quelles étapes pour sortir de la crise et reconstruire son SI ?

- L'**analyse forensique** permet d'identifier et d'isoler les zones compromises (**grey zone**)
- Les zones corrompues sont **reconstruites à l'état de l'art**, sur des bases saines :
  - Restauration des sauvegardes
  - Reconstruction du système d'information
  - Réinstallation des applications
- Une **assistance opérationnelle et juridique** doit être mise en place :
  - Assistance opérationnelle : faire appel aux prestataires cyber de l'entreprise et aux interlocuteurs publics (ANSSI, CSIRT régional, Gendarmerie ou Police) pour obtenir une aide sur-mesure
  - Assistance juridique : faire appel aux assureurs et aux interlocuteurs publics qui pourront conseiller l'entreprise dans la construction du dossier et le parcours de plainte
- L'**effort de communication** doit être maintenu vis-à-vis de l'ensemble des parties prenantes
- L'**accompagnement psychologique** mis en place au cours de la gestion de crise doit être maintenu une fois la crise passée, notamment pour contrer le stress post-traumatique

## Bonnes pratiques opérationnelles

- S'assurer de l'**accessibilité** des fiches réflexes et des plans de reprise de l'activité, et de la **connaissance de leur emplacement (hors SI)** par tous les collaborateurs
- Définir **plusieurs scénarios de PRA** en fonction du type d'incident
- Reconstruire le SI **sur des bases saines**, et non sur la base des infrastructures compromises
- Après la crise, **tirer les enseignements adéquats** : ce qui a fonctionné ou n'a pas fonctionné, quels éléments auraient pu être mieux préparés

## En conclusion
### Que dire demain à ses collaborateurs ?

**À sa direction générale :**

- L'importance de l'**assistance psychologique** et de son maintien après la crise est-elle acquise ?
- Les **rôles de communication** (en interne et en externe) sont-ils bien définis pour permettre l'effort de communication au long cours ?

**À sa DSI :**

- Les différents **plans de reprise d'activité**, à choisir en fonction du scénario, sont-ils établis et accessibles hors du SI ?
- Les **sauvegardes** sont-elles opérationnelles et accessibles ?
- Les **contacts des prestataires cyber** et des divers **contacts d'urgence** (interlocuteurs publics notamment) sont-ils listés et accessibles hors du SI ?

# ANNEXES

# Contacts opérationnels des services de l'État

## *ANSSI : les contacts régionaux*

| Régions | Siège | Référents | Contact |
|---|---|---|---|
| Auvergne-Rhône-Alpes | Lyon | Mathieu DELAPLACE / Marianne DELARUE | auvergne-rhone-alpes[at]ssi.gouv.fr |
| Bourgogne-Franche-Comté | Dijon | Véronique BRUNET | bourgogne-franche-comte[at]ssi.gouv.fr |
| Bretagne | Rennes | Christian CEVAËR | bretagne[at]ssi.gouv.fr |
| Centre-Val-de-Loire | Orléans | Jean-Manuel GAGET | centre-val-de-loire[at]ssi.gouv.fr |
| Corse | Ajaccio | Moïse MOYAL | corse[at]ssi.gouv.fr |
| Grand-Est | Strasbourg | Vincent RHIN | grand-est[at]ssi.gouv.fr |
| Hauts-de France | Lille | Hugo LONGUESPE | hauts-de-france[at]ssi.gouv.fr |
| Ile-de-France | Paris | Guillaume CRÉPIN | ile-de-france[at]ssi.gouv.fr |
| Normandie | Caen | Eric HAZANE | normandie[at]ssi.gouv.fr |
| Nouvelle-Aquitaine | Bordeaux | Olivier GRALL / Martin VERON | nouvelle-aquitaine[at]ssi.gouv.fr |
| Occitanie | Toulouse | Rémy DAUDIGNY / Anne TRICAUD / Christophe FLEURY | occitanie[at]ssi.gouv.fr |
| Provence-Alpes-Côte d'Azur | Marseille | Kevin HEYDON | paca[at]ssi.gouv.fr |
| Pays-de-la-Loire | Nantes | Régis DUBRULLE | pays-de-la-loire[at]ssi.gouv.fr |
| Outre-Mer | Paris | Moïse MOYAL | outre-mer[at]ssi.gouv.fr |

## *En cas d'attaque*

- Le **17** qui orientera vers le bon service
- Le **CERT** : cert-fr@ssi.gouv.fr
- **Cybermalveillance.gouv.fr** pour une orientation en ligne

**Ces contacts et ceux de vos prestataires cyber et assureurs sont à conserver en-dehors du SI, localisable par tous et accessibles en cas de crise.**

# Fiche de poste

## Responsable de la Sécurité des Systèmes d'Information (RSSI)

Extrait du guide ***Panorama des métiers de la cybersécurité***, édition 2020
**Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)**
*Pages 10 à 13*

# RESPONSABLE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI)

**Equivalence en anglais :** *Chief Information Security Officer (CISO), Director of Information Security.*

**Autres titres équivalents :**

- **FR :** Officier de Sécurité des Systèmes d'Information (OSSI), Fonctionnaire de Sécurité des Systèmes d'Information (FSSI), Responsable de la Confiance Numérique (RCN)
- **EN :** *Information System Security Manager (ISSM), Information Security Manager*

## MISSION ESSENTIELLE

Le Responsable de la sécurité des systèmes d'information (RSSI) assure le pilotage de la démarche de cybersécurité sur un périmètre organisationnel et/ou géographique au sein de l'organisation. Il définit ou décline, selon la taille de l'organisation, la politique de sécurité des systèmes d'information (prévention, protection, détection, résilience, remédiation) et veille à son application. Il assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte, en particulier auprès des directeurs métiers et/ou de la direction de son périmètre.

Il s'assure de la mise en place des solutions et des processus opérationnels pour garantir la protection des données et le niveau de sécurité des systèmes d'information. Selon la taille de l'organisation, il joue un rôle opérationnel dans la mise en œuvre de la politique de sécurité des SI ou encadre une équipe.

## ACTIVITÉS ET TÂCHES

| IDENTIFIER |
|---|
| Décliner les axes et les objectifs stratégiques en matière de cybersécurité pour son périmètre et les faire valider par la direction compétente sur celui-ci |
| Identifier les enjeux et les risques de sécurité majeurs sur son périmètre |
| Décliner et maintenir la politique de sécurité des SI en collaboration avec les parties prenantes |
| Définir un plan d'actions annuel ou pluriannuel sur son périmètre |
| Définir une politique d'investissement au regard des objectifs de sécurité |
| Contribuer à définir l'organisation de la cybersécurité au sein de son périmètre et l'animer |
| Suivre les évolutions réglementaires et techniques de son domaine ; assurer les relations avec les acteurs de son secteur d'activité autour de la cybersécurité |

| PROTÉGER |
|---|
| Organiser les structures de pilotage des plans d'actions de sécurité au sein des entités |
| Définir les mesures organisationnelles et techniques à mettre en œuvre pour atteindre les objectifs de sécurité |
| Assurer un support à la mise en œuvre en fournissant une assistance technique et méthodologique ainsi que des outils et services de sécurité, éventuellement à travers un catalogue de services |
| Diffuser une culture SSI à destination des utilisateurs et décideurs |
| Assurer la promotion des chartes de sécurité informatique sur son périmètre |
| Évaluer le niveau de sécurité au sein de son périmètre, notamment à travers la réalisation d'audits périodiques et de contrôles permanents |
| Contrôler que les politiques et règles de sécurité des SI sont appliquées sur son périmètre et vis-à-vis des tiers et sous-traitants (*third parties*) |
| Contribuer à répondre aux sollicitations des prospects et des clients de l'organisation sur les aspects sécurité (notamment dans le cadre d'appels d'offres) |

| DÉTECTER |
| --- |
| Prendre les mesures techniques et/ou organisationnelles permettant la surveillance des événements de sécurité, l'appréciation des incidents de sécurité et la réaction face aux attaques, assurer la mise en place d'un SOC (*Security Operation Center*) |

| RÉPONDRE |
| --- |
| Veiller à ce que le dispositif de gestion de crise de sécurité soit opérationnel |
| Contribuer au pilotage de la gestion des incidents et des crises de sécurité, le cas échéant en lien avec le CSIRT (*Computer Security Incident Response Team*) |

| ASSURER LA CONTINUITÉ ET RECONSTRUIRE |
| --- |
| Préparer et mettre en œuvre un plan de continuité informatique, dans le cadre du plan de continuité des activités (PCA) |
| Préparer et mettre en œuvre un plan de reprise informatique, dans le cadre du plan de reprise des activités (PRA) |
| Proposer la stratégie de cyber-résilience |

| RENDRE COMPTE |
| --- |
| Rapporter régulièrement auprès de sa hiérarchie sur le niveau de couverture courant des risques de sécurité SI |
| Assurer un rôle de conseil auprès de sa hiérarchie et des métiers de son périmètre |
| Représenter l'organisation dans les relations avec les autorités de régulation |

## FORMATION / EXPÉRIENCE PROFESSIONNELLE

| |
| --- |
| Formation : Bac + 5 avec une spécialisation en cybersécurité |
| Expérience professionnelle : supérieure à 5 ans dans le domaine de la cybersécurité |

## COMPÉTENCES

| COMPÉTENCES CŒUR DE MÉTIER |
| --- |
| Bonne connaissance des enjeux et des métiers de l'organisation |
| Capacité à construire la stratégie cybersécurité de l'organisation |
| Capacité de compréhension des menaces cybersécurité |
| Connaissance du système d'information et des principes d'architecture |
| Maîtrise des fondamentaux dans les principaux domaines de la SSI |
| Connaissance des technologies de sécurité et des outils associés |
| Gestion des risques, politique de cybersécurité et SMSI |
| Connaissance juridique en matière de droit informatique lié à la sécurité des SI et à la protection des données |
| Cyberdéfense : connaissances en gestion de crise |
| Connaissance de la gouvernance, des normes et des standards dans le domaine de la sécurité : normes ISO (2700X), normes sectorielles (PCI-DSS…) |

| COMPÉTENCES COMPORTEMENTALES |
| --- |
| Capacité d'influence |
| Sens de l'intérêt général |

| |
|---|
| Management d'équipe |
| Capacité de restitution au management |
| Capacité à travailler en transverse au sein de l'organisation |
| Capacité à résister à la pression |
| Capacité d'appropriation des enjeux métiers |

### TENDANCES ET FACTEURS D'ÉVOLUTION DU MÉTIER

Le périmètre de responsabilité du RSSI peut s'exercer sur différents domaines en fonction de la nature de l'organisation. Dans les organisations comportant des SI industriels, il existe généralement un RSSI pour le périmètre industriel. Dans les organisations qui développent des produits comportant des SI, un RSSI peut être nommé (dans ce cas, on peut parler de *Product Security Officer* (PSO)).

Dans les grandes entreprises ou administrations, les activités et tâches peuvent être réparties entre un Directeur Cybersécurité ou un RSSI Groupe qui porte la responsabilité globale et des Responsables de la Sécurité des SI (RSSI) qui déclinent les actions sur leurs périmètres respectifs.

## Déclinaison pour le Responsable de sécurité des SI au sein d'une PME / TPE

Au sein d'une PME / TPE, la fonction de Responsable de la sécurité des systèmes d'information n'est pas un poste dédié et les missions et activités peuvent être portées par le DSI, le responsable informatique, un administrateur, un exploitant ou bien un responsable de projet informatique.

Les activités et tâches essentielles qui doivent être prises en charge par une ou plusieurs personnes de l'organisation sont décrites ci-dessous.

### ACTIVITÉS ET TÂCHES

| IDENTIFICATION |
|---|
| Identifier les risques de sécurité sur son périmètre |
| Définir et maintenir la politique de sécurité des SI |

| PROTECTION |
|---|
| Définir les mesures organisationnelles et techniques de sécurité, les déployer, en assurer le fonctionnement opérationnel et les maintenir à l'état de l'art |
| S'assurer que les projets sont conçus et menés de manière sécurisée |
| S'assurer que les politiques et règles de sécurité sont appliquées dans l'organisation, piloter les audits de sécurité sur le SI de l'organisation, suivre les actions de remédiation |
| Réaliser le paramétrage et l'administration des outils de sécurité |
| Diffuser une culture SSI à destination des utilisateurs et sensibiliser les décideurs aux problématiques de sécurité |

| DÉTECTION ET RÉPONSE |
| --- |
| Contribuer à la détection et au pilotage de la gestion des incidents et des crises de sécurité |
| Préparer et mettre en œuvre un plan de continuité informatique |

| REPORTING |
| --- |
| Produire des états des actions de sécurité au sein de l'organisation |
| Mobiliser des expertises extérieures si besoin |

Rédigé à partir des recommandations de l'ANSSI