# Module N°1 : Comprendre les cybermenaces des PME

## Livret du participant

- **Objectif : Comprendre pourquoi les PME sont des cibles privilégiées et instaurer les bons réflexes dès le premier jour.**

Ce livret accompagne la première séance du parcours de sensibilisation. Il reprend l'essentiel de ce qui est présenté en diaporama ce jour.

## Table des matières

I. CE QUE VOUS SAUREZ FAIRE À LA FIN DU MODULE....2

II. D'UN HÔPITAL À VOTRE PME....2

2.1. UNE ATTAQUE RÉELLE : LE CENTRE HOSPITALIER SUD-FRANCILIEN....2
2.2. ET DANS UNE PME ?....3

III. POURQUOI UNE PME INTÉRESSE LES ATTAQUANTS....3

3.1. LES ATTAQUES NE VISENT PAS TOUJOURS UNE ENTREPRISE EN PARTICULIER....3
3.2. VOTRE PME PEUT SERVIR DE PORTE D'ENTRÉE VERS UNE AUTRE ENTREPRISE....4
3.3. VOS MOYENS SONT LIMITÉS....4
3.4. CE QUE CHERCHENT LES ATTAQUANTS....5
3.5. QUELQUES CHIFFRES....5
3.6. QUI ATTAQUE....6
3.7. EXEMPLE : UNE PME DE MÉCANIQUE....6

IV. LES QUATRE ATTAQUES À CONNAÎTRE....6

4.1. LE RANÇONGICIEL....6
4.2. L'HAMEÇONNAGE OU PHISHING....8

**4.3. LA FRAUDE AU PRÉSIDENT OU AU FAUX FOURNISSEUR....9**
**4.4. LE VOL OU LA FUITE DE DONNÉES....10**
**4.5. UNE ATTAQUE, ÉTAPE PAR ÉTAPE....11**

**V. MESURER LES DÉGÂTS : D, I, C....11**

**5.1. LA DISPONIBILITÉ....12**
**5.2. L'INTÉGRITÉ....12**
**5.3. LA CONFIDENTIALITÉ....12**
**5.4. TABLEAU RÉCAPITULATIF....13**

**VI. ATELIER PARTICIPATIF : VOTRE PME FACE À UNE CYBERATTAQUE (20 MINUTES)....13**

**6.1. OBJECTIF....13**
**6.2. ORGANISATION....13**
**6.3. SCÉNARIO A : UNE ENTREPRISE PARALYSÉE....13**
**6.4. SCÉNARIO B : UN VIREMENT DÉTOURNÉ....14**
**6.5. SCÉNARIO C : UN FICHIER CLIENTS ACCESSIBLE....14**

**VII. CONCLUSION : CE QU'IL FAUT RETENIR....15**

**VIII. FICHES PRATIQUES....16**

**IX. SOURCES....17**

# I. Ce que vous saurez faire à la fin du module

1. Expliquer pourquoi une PME comme la vôtre intéresse les attaquants.
2. Reconnaître les quatre attaques les plus courantes et leurs signaux.
3. Repérer ce qui est vital dans votre entreprise et ce qu'une attaque lui ferait perdre.
4. Appliquer trois réflexes simples face à une demande suspecte.

# II. D'un hôpital à votre PME

## *2.1. Une attaque réelle : le centre hospitalier Sud-Francilien*

Dans la nuit du 20 au 21 août 2022, le centre hospitalier Sud-Francilien, situé à Corbeil-Essonnes, découvre qu'il est victime d'une cyberattaque majeure.

Une grande partie de son système informatique est devenue inaccessible. Plusieurs services sont perturbés, notamment la messagerie, la pharmacie et la comptabilité. Certains équipements de laboratoire ne fonctionnent plus normalement. Des nouveau-nés doivent être transférés vers d'autres établissements.

Les professionnels de santé doivent adapter leurs pratiques et réorganiser les soins.

Les attaquants, liés au groupe criminel LockBit, réclament une rançon de **10 millions de dollars** pour permettre la récupération des systèmes informatiques.

L'attaque ne se limite pas à un simple blocage : des données sont également dérobées, puis divulguées.

**Question aux participants :** Comment les attaquants ont-ils réussi à pénétrer dans le système informatique de l'hôpital ?

**Question aux participants :** Un hôpital n'est pas une PME. Qu'est-ce qui, selon vous, rendrait votre entreprise intéressante pour un cybercriminel ?

### 2.2. Et dans une PME ?

L'attaque de cet hôpital montre qu'une cyberattaque peut provoquer des conséquences bien au-delà du domaine informatique.

Dans une PME, l'indisponibilité du système de facturation, d'un logiciel de production ou de la messagerie professionnelle peut également empêcher les salariés de travailler.

Un exemple récent, à Angers : Octave, éditeur de logiciels de 38 salariés. À la mi-août 2024, un rançongiciel chiffre une partie de ses systèmes. Chez ses clients, des sites web et des systèmes de magasin tombent en panne.

L'un d'eux, Lyophilise & Co, PME de 20 salariés à Lorient, se retrouve à l'arrêt et perd près de 20 000 euros par jour. Elle recrée un site internet en quatre jours pour repartir. Octave, de son côté, est placée en redressement judiciaire en novembre 2024, puis en liquidation en mars 2025. Une telle issue reste rare, mais elle montre ce qu'une PME peut avoir à perdre.

La question n'est donc pas seulement : « Qui pourrait vouloir attaquer notre entreprise ? », mais aussi : « Qu'avons-nous à perdre si nos outils numériques ne fonctionnent plus ? »

## III. Pourquoi une PME intéresse les attaquants

En 2025, les services de police et de gendarmerie ont enregistré 453 900 crimes et délits liés au numérique. Ces infractions comprennent différentes formes d'escroquerie, de fraude et d'atteintes aux systèmes informatiques. Toutes ne correspondent pas à des intrusions techniques, mais elles témoignent de l'importance des risques liés au numérique.

Beaucoup de dirigeants pensent : « nous sommes trop petits pour intéresser des pirates ». C'est l'inverse. Trois raisons l'expliquent.

## 3.1. Les attaques ne visent pas toujours une entreprise en particulier

Cette idée repose sur une représentation souvent trompeuse : celle d'un attaquant qui choisit personnellement sa victime et prépare pendant plusieurs semaines une intrusion.

Ce scénario existe, mais de nombreuses cyberattaques sont opportunistes.

Les attaquants peuvent utiliser des programmes automatisés qui recherchent des systèmes vulnérables, testent des identifiants compromis ou diffusent des messages frauduleux à grande échelle.

**Prenons un exemple simple.**

Un cybercriminel envoie 50 000 faux courriels imitant un service de livraison. Les messages demandent aux destinataires de cliquer sur un lien et de saisir leurs identifiants professionnels.

Il ne connaît pas nécessairement les entreprises auxquelles il écrit.

Son objectif est de récupérer des comptes exploitables.

Si un salarié communique son mot de passe, l'entreprise devient une victime potentielle.

**Question aux participants :** Pensez-vous qu'un attaquant doit connaître votre entreprise pour réussir à vous voler des données ou de l'argent ?

## 3.2. Votre PME peut servir de porte d'entrée vers une autre entreprise

Une PME travaille rarement de manière isolée.

Elle échange des courriels, des factures, des documents et parfois des accès informatiques avec ses clients, ses fournisseurs ou ses sous-traitants.

Un attaquant peut exploiter ces relations de confiance.

Imaginons une PME qui réalise des prestations informatiques pour un grand groupe industriel :

- Le grand groupe dispose d'un service de cybersécurité, de systèmes de surveillance et de règles strictes.
- La PME, en revanche, possède moins de moyens techniques et humains.

Si l'attaquant parvient à compromettre un compte utilisé par le prestataire, il peut tenter d'exploiter cette relation pour accéder aux systèmes ou aux informations du client.

C'est ce qu'on appelle un **risque lié à la chaîne d'approvisionnement**, ou *supply chain*.

Le risque joue aussi dans l'autre sens : l'attaque d'un prestataire peut arrêter ses clients. Le 12 août 2021, un rançongiciel frappe Solware, éditeur de logiciels installé près de Lyon, qui équipe notamment des garages. Ses sauvegardes sont supprimées et les données de 1 500 garages clients sont chiffrées : ceux qui utilisaient ses logiciels hébergés perdent l'accès à leur outil de gestion.

La directive européenne NIS 2 renforce cette attention portée à la sécurité des fournisseurs et des prestataires pour les entités concernées.

En France, sa transposition est encore en cours en novembre 2026. Les PME n'y sont donc pas encore soumises, et toutes ne le seront pas.

En revanche, certaines entreprises peuvent recevoir des exigences de sécurité de leurs clients, notamment par contrat.

**Question aux participants :**

Votre entreprise échange-t-elle des fichiers confidentiels ou des accès numériques avec des clients ou des prestataires ?

## 3.3. Vos moyens sont limités

Les PME ne disposent pas toujours d'une équipe informatique dédiée.

Leur informatique peut être gérée par un salarié polyvalent, un prestataire externe ou directement par le dirigeant.

Les difficultés les plus fréquentes peuvent être les suivantes :

- Des logiciels qui ne sont pas régulièrement mis à jour.
- Des mots de passe partagés entre plusieurs collaborateurs.
- Des sauvegardes qui existent, mais dont la restauration n'a jamais été testée.
- Des comptes professionnels sans double authentification.
- Des anciens salariés qui conservent certains accès.
- Une absence de procédure clairement définie en cas d'incident.

Il ne s'agit pas de considérer que toutes les PME rencontrent ces problèmes.

En revanche, lorsque plusieurs de ces faiblesses sont présentes, elles augmentent les possibilités d'attaque et les difficultés de récupération.

**À retenir :**

La cybersécurité ne consiste pas nécessairement à acheter des équipements coûteux.

**Elle commence souvent par une bonne organisation, des protections adaptées et des habitudes simples, appliquées régulièrement.**

## 3.4. Ce que cherchent les attaquants

- **L'argent :** détourner le paiement d'une facture ou obtenir une rançon.
- **Les données :** des plans, des informations commerciales, une recette, un fichier de clients.
- **La capacité à produire :** bloquer les outils pour faire pression sur l'entreprise.
- **L'intention de nuire :** saboter un système, dégrader une réputation ou perturber l'activité.

## 3.5. Quelques chiffres

| Le chiffre | Ce qu'il dit |
|---|---|
| **16 %** | des entreprises de moins de 250 salariés déclarent au moins un incident de cybersécurité dans les 12 derniers mois. |
| **43 %** | des entreprises touchées attribuent l'attaque à un hameçonnage (faux courriel, faux SMS, fausse page). |

| Le chiffre | Ce qu'il dit |
|---|---|
| **49 %** | des petites entreprises reconnaissent ne pas être préparées à une attaque, et 31 % ne savent pas si elles le sont. |
| **26 %** | seulement utilisent la double authentification, l'une des protections les plus efficaces (module 2). |
| **+ 170 %** | de demandes d'assistance pour fraude au virement en 2025 auprès de Cybermalveillance.gouv.fr, tous publics confondus. |

Sources : baromètre TPE-PME 2025 de Cybermalveillance.gouv.fr (OpinionWay, 588 entreprises, juin-juillet 2025) ; rapport d'activité 2025 de Cybermalveillance.gouv.fr, mars 2026.

Ces chiffres montrent deux réalités. D'abord, les cyberattaques ne sont pas un risque exclusivement théorique ; ensuite, de nombreuses entreprises reconnaissent ne pas être suffisamment préparées pour y faire face.

**Questions aux participants :**

Parmi ces chiffres, lequel vous surprend le plus ? Pourquoi ?

## 3.6. Qui attaque

| Profil | Ce qu'il cherche |
|---|---|
| **L'amateur** | Tester des outils tout faits, souvent au hasard |
| **L'organisation criminelle** | L'argent, à grande échelle. Elle fonctionne comme une entreprise : développement, support, recrutement d'affiliés |
| **L'activiste** | Faire passer un message, nuire à une image |
| **L'État espion** | Voler un savoir-faire, des informations stratégiques |
| **L'employé mécontent ou l'ex-salarié** | Se venger, emporter des données |
| **Le mercenaire** | Attaquer pour le compte d'un commanditaire |

Pour une PME, trois profils comptent vraiment : **l'organisation criminelle**, qui attaque en masse et sans viser personne en particulier, **la personne de l'intérieur (salarié ou ex-salarié) et l'amateur.**

**Ces profils ne sont pas totalement indépendants. Une organisation criminelle peut, par exemple, employer des personnes qui développent ou louent des outils d'attaque.**

Il ne faut toutefois pas supposer qu'un employé mécontent est nécessairement dangereux.

**La bonne pratique consiste à gérer correctement les droits d'accès de tout le personnel, notamment lors des départs.**

## 3.7. Exemple : une PME de mécanique

Une entreprise de 15 salariés est spécialisée dans la fabrication de pièces mécaniques. Elle possède des plans techniques, des fichiers clients, un logiciel de gestion commerciale et des machines indispensables à sa production.

**Question aux participants :** quels sont les risques encourus ?

# IV. Les quatre attaques à connaître

## 4.1. Le rançongiciel

### a) Définition

Un rançongiciel, ou *ransomware*, est un programme malveillant utilisé pour bloquer l'accès à des systèmes ou à des données.

Dans de nombreuses attaques, les fichiers sont chiffrés : ils deviennent illisibles sans une clé de déchiffrement.

L'attaquant réclame une somme d'argent pour permettre leur récupération.

Dans certains cas, il menace également de publier des documents confidentiels qu'il a dérobés.

### b) Comment le rançongiciel peut-il entrer ?

L'attaquant peut exploiter un accès distant mal protégé, un compte compromis, une vulnérabilité logicielle ou un fichier malveillant.

Il peut également rester un certain temps dans le système avant de déclencher le chiffrement.

### a) Exemple réel : Fondouest (2024)

Le 1er février 2024, en début d'après-midi, tout s'arrête chez Fondouest, bureau d'études géotechniques d'une soixantaine de salariés répartis sur cinq sites dans l'Ouest.

Selon son prestataire informatique, tout est parti de la pièce jointe d'un courriel, ouverte par un collaborateur.

Les huit serveurs, les deux tiers des postes et la téléphonie sont hors service. Sur chaque site, les imprimantes sortent un message en anglais qui réclame une rançon.

**Question aux participants : Quelles peuvent être les conséquences ?**

**La suite.** Fondouest ne paie pas la rançon. Ses sauvegardes, faites très régulièrement, sont intactes : avec son prestataire, elle redémarre au bout de quatre jours, puis travaille une quinzaine de jours en mode dégradé. Coût estimé : environ 75 000 euros de perte d'exploitation et 30 000 euros de prestataires.

**Question aux participants :**

Votre entreprise pourrait-elle travailler pendant quatre jours sans ses serveurs ni sa téléphonie ?

**À retenir :**

**Ce qui se passe.** Un programme malveillant chiffre vos fichiers et vos serveurs : tout devient illisible. Un message réclame une rançon pour les débloquer, et menace souvent de publier vos données.

**Ce que ça coûte.** L'activité s'arrête : plus de devis, plus de factures, plus de production. Pendant des jours, parfois des semaines. Payer ne garantit ni la récupération des fichiers, ni la discrétion.

**Comment il entre.** Le plus souvent par un compte dont le mot de passe a été volé, ou par une pièce jointe piégée ouverte quelques semaines plus tôt.

**Message essentiel : le coût d'un rançongiciel ne se limite pas à la rançon demandée. L'arrêt de l'activité et la reconstruction des systèmes peuvent représenter des pertes très importantes. Payer ne garantit pas la récupération des fichiers.**

## 4.2. L'hameçonnage ou phishing

### a) Définition

L'hameçonnage, ou phishing, consiste à tromper une personne en lui faisant croire qu'elle communique avec un interlocuteur légitime.

L'attaque peut prendre la forme d'un courriel, d'un SMS, d'un message instantané, d'un appel téléphonique ou d'une page Internet frauduleuse.

L'objectif peut être de récupérer des identifiants, de provoquer un paiement ou de faire installer un logiciel malveillant.

### b) Exemple : Une salariée reçoit le message suivant

« Votre mot de passe Microsoft 365 expire aujourd'hui. Pour éviter la suspension de votre compte professionnel, veuillez confirmer immédiatement vos identifiants. »

Le message reprend le logo de Microsoft et présente un bouton « Vérifier mon compte ».

La salariée clique sur le bouton.

Elle arrive sur une page ressemblant à une page de connexion Microsoft, mais cette page appartient en réalité à l'attaquant.

Si elle saisit ses identifiants, ceux-ci peuvent être récupérés.

L'attaquant pourrait ensuite tenter d'accéder à sa messagerie et d'exploiter les informations qu'elle contient.

**Question aux participants : Quels sont les signaux d'alerte ?**

Attention : un message frauduleux peut être très bien rédigé et provenir d'un compte réellement piraté. L'absence de fautes d'orthographe n'est pas une garantie de fiabilité.

**Question aux participants :**

Si vous recevez ce message, comment pouvez-vous vérifier qu'il s'agit d'une véritable demande ?

### c) Exemple réel : André Laurent (2023)

En novembre 2023, chez André Laurent, PME de boulonnerie-visserie proche de Saint-Étienne, une salariée ouvre un courriel frauduleux. L'attaquant récupère son carnet d'adresses professionnel et s'en sert pour envoyer de fausses factures à une quinzaine de clients.

**Question aux participants :**

Comment alerter rapidement quinze clients si une fausse facture leur a été adressée en votre nom ?

**À retenir :**

**Ce qui se passe.** Un faux message (courriel, SMS, QR code) imite une marque connue, votre banque ou un collègue, et vous amène sur une fausse page pour y saisir vos identifiants.

**Ce que ça coûte.** Avec vos identifiants, l'attaquant lit votre messagerie, écrit à vos clients en votre nom, prépare une fraude au virement ou un rançongiciel. C'est la porte d'entrée de presque tout le reste.

**Les signaux.** Une urgence (« avant ce soir »), une menace (« votre compte sera supprimé »), un lien dont l'adresse ne correspond pas tout à fait au site attendu.

**Message essentiel : un message soigné n'est pas une garantie. Au moindre doute, mieux vaut passer par le service habituel que par le lien reçu.**

## 4.3. La fraude au président ou au faux fournisseur

### a) Définition

Cette attaque vise principalement à obtenir un transfert d'argent par tromperie.

Le cybercriminel usurpe l'identité d'une personne connue ou considérée comme légitime.

Il peut se faire passer pour un dirigeant, un responsable financier, un fournisseur ou un partenaire commercial.

### b) Exemple 1 : La fraude au président

Une comptable reçoit un message semblant provenir du directeur :

« Nous devons effectuer aujourd'hui un virement confidentiel de 18 500 euros dans le cadre d'une opération urgente. Merci de ne pas en parler et de m'envoyer la confirmation dès que le paiement sera effectué. »

Le message utilise le nom et parfois l'adresse réelle du dirigeant, si son compte a été compromis.

L'attaquant cherche à exploiter l'autorité hiérarchique, l'urgence et la confidentialité.

**Un cas réel.** À l'été 2015, chez BRM Mobilier, fabricant de mobilier pour bibliothèques à Bressuire (Deux-Sèvres), des escrocs se font passer pour le PDG. Ils écrivent à la comptable et obtiennent, pour une opération présentée comme très confidentielle, une série de virements vers l'Asie : 1,6 million d'euros en quelques semaines. L'entreprise, qui employait 44 salariés, est placée en redressement judiciaire en septembre 2015, puis en liquidation en janvier 2016.

### c) Exemple 2 : Le faux fournisseur

Une entreprise travaille depuis plusieurs années avec le même fournisseur.

Elle reçoit un courriel annonçant un changement de coordonnées bancaires et demandant de régler les prochaines factures sur un nouveau RIB.

Le courriel reprend l'identité visuelle du fournisseur. Il peut même s'insérer dans une conversation professionnelle existante si une messagerie a été piratée.

La comptabilité modifie les coordonnées bancaires et réalise le paiement.

L'argent est alors envoyé sur le compte contrôlé par l'escroc.

**Question aux participants : Quels sont les signaux d'alerte ?**

**Question aux participants :**

Un fournisseur vous informe par courriel qu'il a changé de banque. Que faites-vous avant de modifier ses coordonnées ?

**À retenir :**

**Ce qui se passe.** Quelqu'un se fait passer pour votre dirigeant (« virement urgent et confidentiel ») ou pour un fournisseur habituel (« nous avons changé de banque, voici notre nouveau RIB »).

**Ce que ça coûte.** L'argent part sur le compte de l'escroc. S'il n'est pas bloqué dans les heures qui suivent, il est souvent perdu.

**Les signaux.** Un changement de coordonnées bancaires, une demande de secret, une pression sur les délais, un interlocuteur qu'on ne peut pas rappeler.

**Message essentiel : une vérification indépendante peut suffire à empêcher un détournement de fonds.**

## 4.4. Le vol ou la fuite de données

### a) Définition

Toutes les cyberattaques ne cherchent pas à bloquer les systèmes informatiques.

Certaines visent à récupérer des informations.

Une PME peut conserver de nombreuses données sensibles :

- Des fichiers clients et fournisseurs.
- Des coordonnées bancaires.
- Des données concernant les salariés.
- Des contrats commerciaux.
- Des plans de fabrication.
- Des informations sur les produits ou les procédés industriels.

### b) Exemple réel : Le Slip Français (2024)

Le 15 avril 2024, Le Slip Français, marque française de textile qui vend en ligne, apprend que des données de ses clients ont été volées : noms, coordonnées et, pour certains, numéros de commande.

Les mots de passe et les données de carte bancaire ne sont pas concernés. Mais les données volées peuvent servir à préparer des courriels, des SMS ou des appels frauduleux visant les clients.

**Question aux participants : Quelles sont les conséquences possibles ?**

**La suite.** L'entreprise prévient ses clients, dépose plainte et signale l'incident à la CNIL.

### c) Lien avec le RGPD

Lorsqu'un incident concerne des données personnelles, l'entreprise doit l'analyser et le documenter.

Si cette violation présente un risque pour les droits et libertés des personnes, le responsable de traitement doit la notifier à la CNIL dans les meilleurs délais et, si possible, dans les 72 heures après en avoir pris connaissance.

En cas de risque élevé, il peut aussi être nécessaire d'informer les personnes concernées.

Toutes les fuites de données ne donnent donc pas automatiquement lieu à une notification à la CNIL.

**Question à se poser :**

> Quelles sont les informations conservées par votre entreprise que vous ne souhaiteriez surtout pas voir publiées sur Internet ?

**À retenir :**

**Ce qui se passe.** Vos fichiers clients, vos plans, vos devis ou les données de vos salariés sont copiés, puis revendus ou publiés.

**Ce que ça coûte.** La confiance de vos clients, parfois le client lui-même. Et des obligations légales : une fuite de données personnelles doit être déclarée à la CNIL sous 72 heures si elle présente un risque pour les personnes.

**Message essentiel : une entreprise n'est pas uniquement intéressante pour son chiffre d'affaires ou sa notoriété. Elle peut l'être pour les informations qu'elle détient, les services qu'elle assure et les entreprises avec lesquelles elle travaille.**

## *4.5. Une attaque, étape par étape*

*Scénario fictif, construit à partir de faits courants, dans une PME agroalimentaire.*

| Étape | Ce que fait l'attaquant | Où un salarié peut casser la chaîne |
|---|---|---|
| **1. Repérage** | Il lit le site de l'entreprise et les profils publics : nom du responsable achats, fournisseur d'emballages | Ce qu'on publie sur soi et sur son poste |
| **2. Préparation** | Il crée une adresse qui imite celle du fournisseur | |
| **3. Envoi** | Courriel au service comptable : « nouveau RIB, merci d'en tenir compte dès la prochaine échéance » | Le doute : un changement de RIB se vérifie toujours par téléphone |
| **4. Exploitation** | Le RIB est modifié dans le logiciel de paiement | La double validation des changements de coordonnées bancaires |
| **5. Installation** | Aucune : pas de logiciel malveillant, seulement une manipulation | |
| **6. Contrôle** | Il surveille les échanges et relance si besoin | Un fournisseur qui réclame un paiement déjà parti |
| **7. Action** | Deux factures réglées sur le mauvais compte | Le signalement immédiat à la banque, qui peut parfois bloquer les fonds |

✓ **<u>Question aux participants :</u> À quelle étape était-il le plus simple d'arrêter l'attaque, et comment ?**

# V. Mesurer les dégâts : D, I, C

Pour comprendre les conséquences d'une cyberattaque, on peut utiliser trois notions fondamentales de la sécurité informatique :

**Disponibilité : Intégrité : Confidentialité**

Ces trois critères constituent ce que l'on appelle le modèle DIC.

Ils permettent de comprendre ce qu'une attaque peut dégrader et d'identifier les éléments à protéger en priorité.

## 5.1. La disponibilité

La disponibilité correspond à la possibilité d'accéder aux informations et aux services lorsqu'on en a besoin.

**Question : puis-je encore travailler ?**

- Reprenons le cas de Fondouest : ses huit serveurs sont bloqués par un rançongiciel.
- Même si les informations n'ont pas été supprimées, les salariés ne peuvent plus les consulter.
- L'entreprise peut alors se trouver dans l'impossibilité de facturer, de produire ou de répondre à ses clients.
- La disponibilité est donc directement liée à la continuité de l'activité.

## 5.2. L'intégrité

L'intégrité correspond au fait que les informations restent exactes, complètes et non modifiées sans autorisation.

**Question : puis-je encore faire confiance à mes informations ?**

- En mai 2023, un pirate modifie la page de paiement de Boutique-rhum.com, un site de vente en ligne : il remplace l'IBAN de l'entreprise par le sien.
- Le site reste en ligne et des clients continuent de commander.
- Pourtant, une information essentielle a été modifiée.
- Les paiements des clients partent vers le compte du pirate, jusqu'à ce qu'un robot de surveillance du site signale l'anomalie.
- C'est une atteinte à l'intégrité.

## 5.3. La confidentialité

La confidentialité consiste à empêcher les personnes non autorisées d'accéder à certaines informations.

**Question : qui peut voir mes données ?**

- Reprenons le cas du Slip Français.
- À la suite d'un piratage, des données de ses clients sont copiées par des attaquants.
- Les fichiers d'origine peuvent très bien rester accessibles et intacts.
- Pourtant, des tiers non autorisés peuvent désormais consulter ces données.
- C'est une atteinte à la confidentialité.

### 5.4. Tableau récapitulatif

Pour savoir ce qu'une attaque fait perdre à votre entreprise, posez trois questions. Elles serviront pendant l'atelier.

| Lettre | La question | Exemple d'attaque qui la touche |
|---|---|---|
| **D : Disponibilité** | Puis-je encore travailler ? Mes outils et mes fichiers sont-ils accessibles ? | Rançongiciel : serveur bloqué, production à l'arrêt |
| **I : Intégrité** | Puis-je encore faire confiance à mes informations ? Quelqu'un a-t-il pu les modifier ? | Faux fournisseur : RIB remplacé dans la fiche fournisseur |
| **C : Confidentialité** | Qui peut voir mes données ? Des personnes non autorisées y ont-elles eu accès ? | Fuite des plans d'un client, messagerie piratée |

**Point important :** une même attaque peut affecter plusieurs critères.

Un rançongiciel qui chiffre les serveurs et dérobe des documents porte atteinte à la disponibilité et à la confidentialité. Il peut également porter atteinte à l'intégrité si des fichiers sont modifiés.

## VI. Atelier participatif : Votre PME face à une cyberattaque

### 6.1. Objectif

Analyser un incident, comprendre ses conséquences et proposer les premières mesures adaptées.

### 6.2. Organisation

Vous travaillez en trois groupes. Chaque groupe reçoit une situation différente.

**3 minutes :** découverte du scénario.

**7 minutes :** analyse en groupe.

**8 minutes :** restitution et correction collective.

**2 minutes :** synthèse.

### 6.3. Scénario A : Une entreprise paralysée

Une entreprise de 20 salariés fabrique des équipements industriels.

Lundi matin, plusieurs collaborateurs ne peuvent plus accéder au serveur contenant les dossiers de fabrication, les devis et les factures.

Un message réclame une rançon en échange du rétablissement de l'accès aux fichiers.

Les salariés indiquent que la dernière sauvegarde vérifiée date de plusieurs semaines.

**Questions :**

1. De quel type d'attaque s'agit-il probablement ?

2. Quels sont les éléments de l'entreprise concernés ?
3. Quels critères DIC sont touchés ?
4. Quelles conséquences peut subir l'entreprise ?
5. Quelles sont les premières actions à envisager ?

## 6.4. Scénario B : Un virement détourné

Une PME reçoit un courriel apparemment envoyé par un fournisseur habituel.

Ce fournisseur annonce un changement de coordonnées bancaires et demande de régler une facture de 12 000 euros sur son nouveau compte.

La comptable effectue le virement sans contacter le fournisseur.

Trois jours plus tard, celui-ci réclame le paiement de sa facture : il n'a jamais changé de banque.

**Questions :**

1. Quel type de fraude reconnaissez-vous ?
2. Quelle information a été falsifiée ?
3. Quel critère DIC est concerné ?
4. Quelles sont les conséquences possibles ?
5. Quelle vérification aurait permis de réduire le risque ?

## 6.5. Scénario C : Un fichier clients accessible

Une entreprise de services conserve un tableau contenant les noms, adresses électroniques, numéros de téléphone et historiques de commandes de ses clients.

Un collaborateur découvre que le fichier est accessible depuis Internet grâce à un lien de partage qui n'exige aucune authentification.

Le lien circule depuis plusieurs jours.

**Questions :**

1. De quel type d'incident s'agit-il ?
2. Quelles données sont concernées ?
3. Quel critère DIC est principalement touché ?
4. Quelles conséquences sont possibles ?
5. Que devrait faire l'entreprise après cette découverte ?

**Vos réponses (scénario de votre groupe) :**

.....

.....

.....

.....

.....

.....

**Notes pendant la restitution :**

.....

.....

.....

.....

# VII. Conclusion : Ce qu'il faut retenir

Les cyberattaques ne concernent pas uniquement les grandes entreprises.

Une PME peut être victime d'une attaque opportuniste, d'une fraude ciblée ou de la compromission d'un système utilisé dans ses relations commerciales.

Les cybercriminels peuvent rechercher de l'argent, des données, un moyen de faire pression sur l'entreprise ou un accès à ses partenaires.

Les quatre grandes menaces étudiées sont :

1. Le rançongiciel.
2. L'hameçonnage.
3. La fraude au président ou au faux fournisseur.
4. Le vol ou la fuite de données.

Pour comprendre leurs conséquences, nous avons identifié trois critères : **disponibilité, intégrité et confidentialité**.

Ces critères permettent de répondre à trois questions fondamentales :

- Puis-je encore travailler ?
- Puis-je encore faire confiance à mes informations ?
- Qui peut voir mes données ?

Et face à une demande inhabituelle, trois réflexes : **je doute, je vérifie par un autre canal, je signale**.

### Dernière question aux participants

**Si vous deviez identifier aujourd'hui un seul élément numérique dont la perte ou l'indisponibilité mettrait votre activité en difficulté, lequel choisiriez-vous ?**

Notez votre réponse :

.....

.....

Cette réponse servira de point de départ pour identifier les mesures de protection prioritaires dans les prochains modules.

**Message final :**

**La cybersécurité ne consiste pas à supprimer tous les risques, ce qui est impossible. Elle consiste à les connaître, à réduire les possibilités d'attaque et à limiter leurs conséquences sur l'activité de l'entreprise.**

# VIII. Fiches pratiques

### a) J'ai cliqué, chef !

Tout le monde peut se faire piéger, y compris les spécialistes. Ce qui fait la différence, c'est ce qu'on fait juste après.

| Ce qui s'est passé | Ce que je fais tout de suite |
|---|---|
| **J'ai cliqué sur un lien, sans rien saisir** | Je ferme la page et je préviens la personne désignée |
| **J'ai saisi un mot de passe** | Je le change immédiatement depuis un autre appareil, partout où je l'utilisais, et je préviens |
| **J'ai ouvert une pièce jointe ou installé quelque chose** | Je débranche l'appareil du réseau sans l'éteindre, et j'alerte |
| **J'ai répondu, donné une information ou validé un paiement** | Je préviens la direction immédiatement ; pour un virement, la banque est appelée dans l'heure pour demander un rappel des fonds |

**Personne ne vous reprochera d'avoir signalé.**
Une erreur signalée en dix minutes se répare. Une erreur cachée pendant une semaine peut coûter très cher à l'entreprise.

### b) Les trois réflexes à retenir

**Face à une demande inhabituelle, quel que soit le canal**

**1. Je doute.** Urgence, autorité inhabituelle, demande de secret : c'est le signal d'arrêt.

**2. Je vérifie par un autre canal.** Je rappelle la personne au numéro que je connais déjà, jamais à celui donné dans le message.

**3. Je signale.** À la personne désignée dans mon entreprise, tout de suite, même si je ne suis pas sûr.

**Dans mon entreprise, je signale à :**

.....

### c) En cas d'incident : qui appeler

| Situation | Contact |
|---|---|
| **Toute cyberattaque, pour un diagnostic et une orientation** | 17cyber.gouv.fr : service public gratuit, 24 h/24, 7 j/7 |
| **Besoin d'une aide technique** | Un prestataire labellisé, trouvé via Cybermalveillance.gouv.fr |
| **Virement frauduleux** | Votre banque, immédiatement, pour tenter de bloquer les fonds ; puis dépôt de plainte |
| **Fuite de données personnelles** | Déclaration à la CNIL sous 72 heures si la fuite présente un risque pour les personnes |
| **Vous avez une cyber-assurance** | Votre assureur, avant d'engager des frais ; plainte à déposer dans les 72 heures, sans quoi l'assurance n'indemnise pas |

Dans tous les cas : ne payez pas de rançon sans avoir pris conseil, n'éteignez pas les machines touchées (débranchez-les du réseau) et notez ce que vous avez vu et à quelle heure.

# IX. Sources


- ANSSI : État de la menace informatique dans le secteur de la santé (2024) : attaque du centre hospitalier Sud-Francilien.
- ARS Île-de-France : Table ronde « PUI, faire face à une cyberattaque » (2023) : pharmacie de l'hôpital.
- LeMagIT : Centre hospitalier Sud-Francilien : ce que dit l'autopsie de la cyberattaque (2022) : mode d'entrée des attaquants.
- Cas Octave et Lyophilise & Co : Clubic (2025) ; Le Journal des Entreprises (2024).
- Cas Solware : Journal Auto (2022).
- Cas Fondouest : CCI France (2024) ; Ouest-France (2024).
- Cas André Laurent : Le Parisien (2024).

- Cas BRM Mobilier : ICI, ex-France Bleu (2016) ; cour d'appel de Poitiers (2025).
- Cas Le Slip Français : communiqué de l'entreprise (2024).
- Cas Boutique-rhum.com : Clubic, d'après Le Parisien (2024).
- Cybermalveillance.gouv.fr : Baromètre TPE-PME 2025 : incidents, préparation, double authentification et hameçonnage.
- Cybermalveillance.gouv.fr : Rapport d'activité 2025 : fraude au virement et tendances.
- Ministère de l'Intérieur : Bilan statistique 2025 : chiffres révisés des infractions numériques.
- CNIL : Notification des violations de données personnelles : obligations RGPD.
- ANSSI : NIS 2 et préparation des organisations : périmètre et situation réglementaire.