Mieux appréhender la CyberSécurité dans l'entreprise

DUOTECH 2025

Sommaire

L’évènement CyberSécurité

DUOTECH, ce sont

Les Services Managés,
La CyberSécurité,
La Comptabilité, la Paie, la Gescom, etc.
La Téléphonie, et la fibre,
L'Infrastructure réseau, Informatique, et le Cloud,
La Digitalisation, et la Dématérialisation,
La Business Intelligence, et le Reporting,
Et la formation (Référent Action de Formation QUALIOPI).

DUO tech INFORMATIQUE

Faisons équipe

Nos équipes de 34 collaborateurs, apportent au quotidien à tous nos utilisateurs une sérénité à travers nos services de supervision, d'infogérance et notre méthode de management de projets informatiques.

DUOTECH, c’est aussi

Reboot2Life propose la location ou l’achat de matériel informatique reconditionné, offrant une solution : **Écologique**, **économique** et **pratique**.

Reboot2Life allie performance, durabilité et simplicité pour un avenir numérique responsable.

Découvrez le PC ÉcoÉvolutif :
La solution permettant : d’upgrader, et d’interchanger l’ensemble du PC.

Reboot 2Life
PRODUITS IT DE SECONDE VIE

Quelques chiffres clés

38 % des professionnels de la sécurité estiment que les attaques par ransomwares seront encore plus dangereuses grâce à l'IA.

Seulement **29 %** des professionnels affirment être « *très bien préparés* » aux attaques de type ransomware.

89 % des personnes interrogées déclarent que la cybersécurité est discutée au sein de l'entreprise.

91 % disent que la cybersécurité est considérée comme une question stratégique majeure dans leur entreprise.

62 % déclarent être mieux préparés à lutter contre les attaques de cybersécurité contrairement à l'année passée.

Environ **22 %** seulement des organisations prévoient d'**augmenter leurs investissements** en gestion de l'exposition en 2025, et 2026.

Source : Rapport d'Ivanti 2025

État de la menace Cyber 2025

Sur 2025, une utilisation toujours accrue de l'intelligence artificielle. Les cybercriminels exploitent l'IA et outil génératifs pour améliorer leurs techniques, comme la création de malwares, la personnalisation des campagnes de phishing ou le « *bruteforce* » de mots de passe via des outils de plus en plus performant. Cela rend les attaques de plus en plus crédibles et efficaces.

Les menaces détectées sur une période de 30 jours en moyenne !

90 % des violations de données impliquent des erreurs humaines.

85 % des cyberattaques exploitent l'IA pour créer des malwares et campagne de phishing.

Types de menaces 1

Malwares : Un malware est un programme ou un code informatique conçu pour nuire à un ordinateur, un réseau ou à ses utilisateurs.

Phishing (ou hameçonnage en français) est une technique de fraude utilisée par des pirates pour voler des informations personnelles - comme des mots de passe, numéros de carte bancaire ou identifiants de connexion.

Le Spear Phishing (ou hameçonnage ciblé) est une forme de phishing très ciblée. Contrairement au phishing “de masse” qui envoie le même faux message à des milliers de personnes, le spear phishing vise une personne ou un petit groupe précis, après avoir collecté des informations sur la cible pour rendre l’attaque crédible.

Un spam, c’est tout simplement un message non sollicité envoyé en grand nombre, souvent à des fins publicitaires ou frauduleuses.

Une attaque DDoS (pour Distributed Denial of Service, ou attaque par déni de service distribué en français) est une attaque informatique qui vise à rendre un site web, un serveur ou un service en ligne indisponible.

Types de menaces 2

L’attaque par les mots de passe est une tentative d’un pirate pour deviner, voler ou casser un mot de passe afin d’accéder à un compte, un ordinateur ou un réseau. C’est l’une des attaques les plus courantes, car beaucoup de gens utilisent encore des mots de passe faibles ou les réutilisent sur plusieurs sites.

Une attaque sur une faille de logiciel (ou exploitation d’une vulnérabilité) consiste à tirer parti d’un défaut dans un programme pour faire faire au logiciel quelque chose qu’il ne devrait pas faire. Autrement dit : le pirate trouve une porte dérobée (la faille) et l’utilise pour pénétrer, perturber ou prendre le contrôle d’un système.

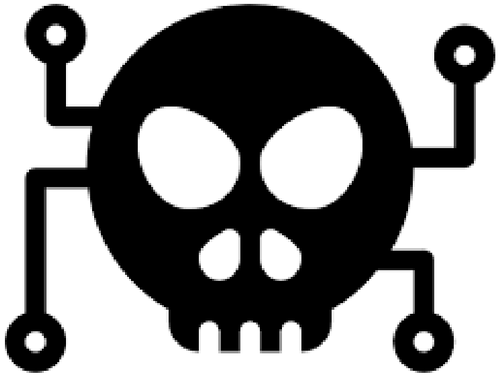
Menaces internes : En cybersécurité, une menace interne (ou *insider threat* en anglais) désigne un risque qui vient de l’intérieur de l’entreprise - c’est-à-dire d’une personne autorisée à accéder au système (employé, prestataire, partenaire, stagiaire, etc.) - mais qui utilise cet accès de manière malveillante ou négligente.

Intelligence Artificielle, etc.

Malware

Un malware est un programme ou un code informatique conçu pour nuire à un ordinateur, un réseau ou à ses utilisateurs. Il peut :

- voler des données personnelles (mots de passe, numéros de carte bancaire, etc.),
- détruire ou chiffrer des fichiers,
- espionner les activités d'un utilisateur,
- ou encore prendre le contrôle d'un système à distance.



Exemples de malwares :

- Virus : s'attache à d'autres fichiers pour se propager.
- Cheval de Troie (Trojan) : semble inoffensif, mais ouvre une porte à des pirates.
- Ransomware : bloque vos données et demande une rançon.
- Spyware : espionne votre activité.
- Worm (ver) : se propage automatiquement d'un ordinateur à un autre.

Phishing

Le phishing : Le terme vient de "*fishing*" (pêcher), car les pirates "pêchent" leurs victimes avec de faux messages qui semblent venir de sources fiables (banques, administrations, services connus comme PayPal, Amazon, etc.).

Comment ça se présente ? Souvent sous la forme de :

- Courriels ou SMS imitant un vrai organisme,
- Faux sites web qui ressemblent à ceux de votre banque ou d'un service officiel,
- Messages sur les réseaux sociaux demandant de "vérifier votre compte" ou de "confirmer un paiement".

Exemple typique : "*Votre compte bancaire a été bloqué pour des raisons de sécurité. Cliquez ici pour le réactiver.*" En cliquant, la victime arrive sur un **faux site** où elle entre ses identifiants - qui sont ensuite envoyés aux pirates.

Comment s'en protéger :

- Ne jamais cliquer sur un lien suspect - Vérifier l'adresse de l'expéditeur.
- Ne pas fournir d'informations personnelles par courriel ou SMS.
- Aller directement sur le site officiel en tapant l'adresse soi-même.
- Utiliser un antivirus et activer la double authentification sur ses comptes.

Spear Phishing

En quoi ça diffère du phishing classique ? Message personnalisé, basé sur des informations réelles (nom, poste, collègues, projets), conçu pour tromper précisément la victime.

Exemples concrets : Un courriel semblant venir du directeur financier demandant un virement urgent vers un nouveau compte ou un message à un collaborateur RH reprenant le nom d'un employé et demandant des bulletins de salaire.

Signes qui doivent alerter :
Le message contient des données personnelles (projets, noms, dates) mais demande quelque chose d'inhabituel.
Urgence et pression pour agir vite.
Destinataire pressenti (vous) mais adresse courriel légèrement différente ou domaine inconnu.
Pièce jointe suspecte ou lien qui redirige vers un site non officiel.
Demande de transmettre des identifiants ou d'effectuer un paiement sans validation par un autre canal.

Comment s'en protéger :
Vérifier via un autre canal (appel ou message à un numéro officiel) avant d'exécuter une demande sensible.
Activer la double authentification (MFA) sur comptes importants.
Former les équipes à repérer les attaques ciblées.

Spam

Le spam = **“courrier indésirable”,** C’est l’équivalent du **prospectus** dans ta boîte aux lettres… mais version numérique.

Où trouve-t-on des spams ?
Courriels : publicités douteuses, arnaques, offres “trop belles pour être vraies”.
SMS : messages pour des “gains” ou de faux colis.
Réseaux sociaux : messages privés automatiques.
Commentaires en ligne : liens vers des sites louches.

Objectifs des spammeurs
Faire de la publicité pour un produit ou un site.
Diffuser des malwares (via des liens ou pièces jointes).
Tromper les gens (phishing, escroqueries, etc.).
Récupérer de l’argent ou des informations personnelles.

Comment s’en protéger ? = Ne jamais répondre à un spam.
Ne jamais cliquer sur un lien ou une pièce jointe douteuse.
Utiliser un filtre anti-spam (la plupart des messageries en ont).
Masquer ton adresse électronique sur les sites publics.
Utiliser plusieurs adresses (Une perso, une pour les inscriptions en ligne).

Attaque DDoS

Comment ça fonctionne ? Imagine qu'un site web est comme un magasin : il peut accueillir un certain nombre de clients à la fois. Lors d'une attaque DDoS, des milliers (ou millions) d'ordinateurs, souvent infectés par un malware, se connectent en même temps au même site. Résultat : le site est saturé et ne peut plus répondre aux vrais utilisateurs.

Détails techniques :
Les pirates utilisent un réseau d'ordinateurs infectés (appelé botnet) pour lancer l'attaque.
Ces ordinateurs peuvent appartenir à n'importe qui, souvent sans que leur propriétaire le sache.
L'attaque inonde le serveur de requêtes jusqu'à ce qu'il plante ou devienne très lent.

Les objectifs possibles : Paralyser un site (souvent pour nuire à une entreprise, une institution ou un concurrent), faire du chantage ("Payez sinon on continue l'attaque"), etc.

Les conséquences : Site ou service indisponible pendant plusieurs heures ou jours, pertes financières importantes, atteinte à la réputation de l'entreprise, et un surcroît de charge pour les équipes techniques.

Moyens de se protéger : Utiliser un pare-feu anti-DDoS ou un service de protection spécialisé, surveiller le trafic pour repérer les pics anormaux, distribuer les serveurs (répartition de charge), etc.

Mot de passe 1

Les principaux types d’attaques par mots de passe :

Attaque par force brute : Le pirate essaie toutes les combinaisons possibles jusqu’à trouver le bon mot de passe. Exemple : a, aa, aaa, abc, abcd, etc. Très longue, mais efficace si le mot de passe est court.

Attaque par dictionnaire : Le pirate utilise une liste de mots courants ou de mots de passe connus (123456, azerty, password, etc.) pour tenter sa chance. Beaucoup de comptes tombent à cause de ça !

Attaque par ingénierie sociale : Le pirate trompe la victime pour qu’elle révèle elle-même son mot de passe (ex : via un faux email de phishing, un appel, ou un site frauduleux). Ici, ce n’est pas la technique qui est attaquée, mais l’humain.

Vol de base de données : Les pirates piratent un site pour voler une base de données d’utilisateurs contenant des mots de passe hachés. Ensuite, ils essaient de “craquer” ces mots de passe à l’aide d’outils spécialisés.

Attaque par réutilisation de mots de passe : Si un mot de passe d’un site piraté est réutilisé ailleurs, les pirates essaient le même identifiant/mot de passe sur d’autres services (banques, réseaux sociaux, etc.).

Mot de passe 2

Comment s’en protéger :

- Utiliser des mots de passe forts : longs, avec lettres, chiffres et symboles.
- Ne jamais réutiliser le même mot de passe sur plusieurs sites.
- Activer la double authentification (2FA) partout où c’est possible.
- Changer immédiatement un mot de passe si un site a été piraté.

Utiliser un gestionnaire de mots de passe

Un **gestionnaire de mots de passe** est un outil qui stocke, protège et gère automatiquement tous tes mots de passe. Il sert à te simplifier la vie tout en renforçant ta sécurité.

Son utilité principale :

Stocker tes mots de passe en toute sécurité, remplir automatiquement les identifiants

Créer des mots de passe très forts : Il peut générer automatiquement des mots de passe longs et complexes, impossibles à deviner. **Exemple : D$7m!aT9qL2x@r**

Éviter la réutilisation des mots de passe

Synchroniser sur tous tes appareils

T’avertir si un mot de passe est compromis

Failles logicielles

Comment ça se passe ?

Découverte de la faille : il peut s'agir d'un bug dans le code, d'une mauvaise configuration, d'un module tiers non mis à jour, etc.

Création d'un exploit : le pirate écrit un morceau de code ou envoie des requêtes spécialement construites pour exploiter la faille.

Exécution de l'attaque : l'exploit permet par exemple d'exécuter du code à distance, d'élever ses privilèges, de lire ou modifier des données, ou de provoquer un déni de service.

Objectif atteint : vol de données, installation de malware, prise de contrôle d'un serveur, effacement de fichiers, etc.

Comment se protéger ?

- Appliquer les mises à jour/patches dès que possible - Pare-feu pour bloquer les requêtes malveillantes.
- Limiter les privilèges : principe du moindre privilège - Scanner régulièrement les vulnérabilités.
- Validation et assainissement des entrées (ne jamais faire confiance aux données utilisateurs).
- Sauvegardes régulières et plans de reprise d'activité, etc.

Menaces internes 1

Les différents types de menaces internes :

L'interne malveillant (intentionnel) : C'est une personne qui agit volontairement pour nuire à l'entreprise. Exemples : Vol de données sensibles avant de quitter l'entreprise, etc.

L'interne négligent (non intentionnel) : Ce n'est pas un pirate, mais ses erreurs ou imprudences créent des failles de sécurité. Exemples : Cliquer sur un lien de phishing, envoyer un fichier confidentiel au mauvais destinataire, laisser un ordinateur sans verrouillage, etc.

Le tiers de confiance compromis : Il s'agit d'un fournisseur, sous-traitant ou prestataire qui a accès au réseau de l'entreprise et devient le vecteur d'une attaque. Exemple : un prestataire informatique dont le compte est piraté permet l'accès au système interne.

Les conséquences possibles :

- Vol ou fuite de données sensibles (clients, finances, R&D)
- Dommages à la réputation de l'entreprise.
- Perte d'argent ou d'avantage concurrentiel
- Perturbation ou blocage de la production.
- Problèmes juridiques (RGPD, confidentialité, contrats).

Menaces internes 2

Comment s’en protéger ?

Appliquer le principe du moindre privilège
= donner à chacun uniquement les accès nécessaires à son travail.

Surveiller les activités internes
= via des journaux (logs), détections d’anomalies, alertes d’accès inhabituels.

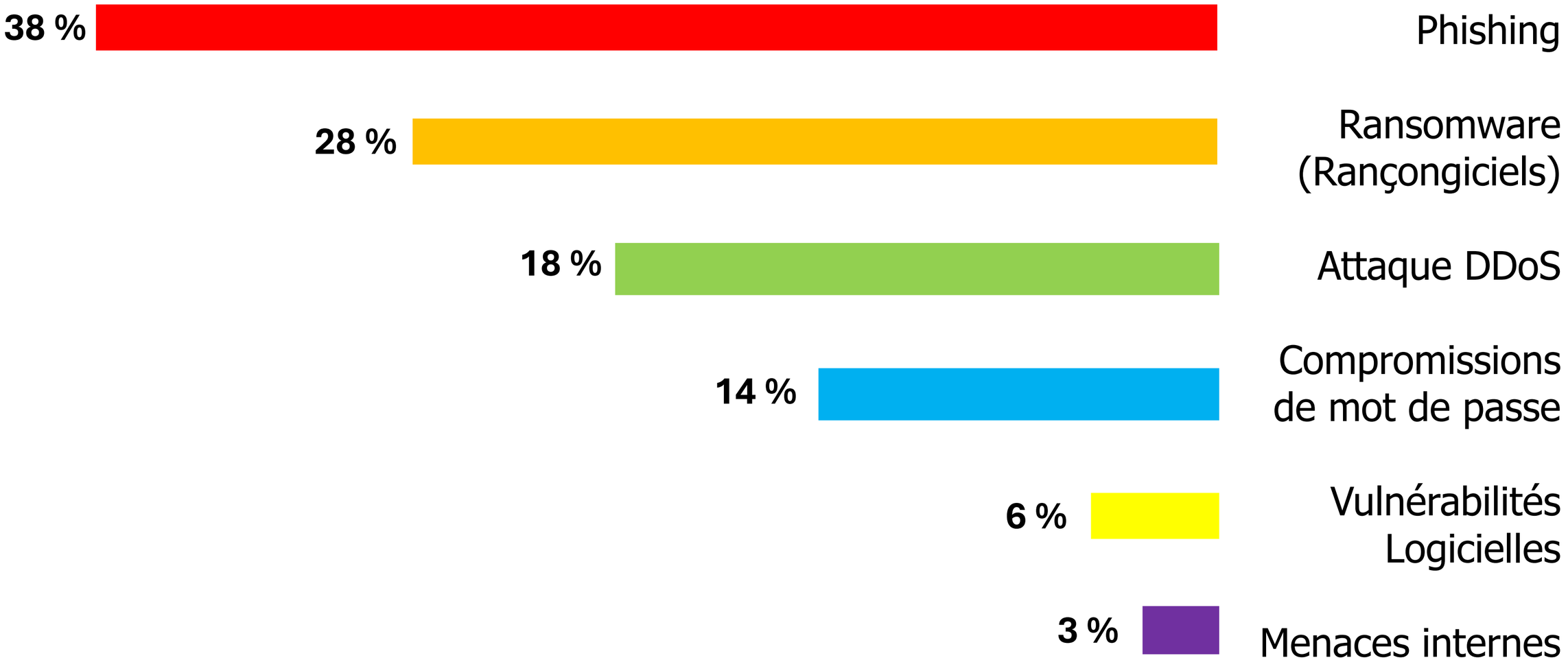
Former le personnel
= à reconnaître les courriels suspects, gérer les mots de passe, et signaler les incidents.

Séparer les comptes et droits d’administration
= éviter qu’une seule personne ait tous les pouvoirs.

Contrôler les accès lors des départs
= désactiver immédiatement les comptes et badges des ex-employés.

Encourager la confiance et le dialogue
= beaucoup d’incidents internes viennent de frustrations ou d’incompréhensions.

Classement de la menace Cyber 2025



Source : Palo Alto Networks 2025 et IBM Cost of a Data Breach Report 2025

Se protéger avec 12 pratiques essentielles

1. Sécuriser et choisir avec soin ses mots de passe
2. Mettre à jour régulièrement vos logiciels et correctifs
3. Vérifier fréquemment les comptes utilisateurs à privilèges
4. Effectuer des sauvegardes régulières
5. Sécuriser et segmenter le réseau de votre entreprise
6. Sécuriser les postes de travail (USB, inactivité...)
7. Protéger ses données lors de ses déplacements, avec un filtre de confidentialité
8. Former régulièrement les employés sur la Cybersécurité (messagerie, mot de passe, jeu ludique)
9. Télécharger ses programmes sur les sites officiels des éditeurs
10. Être vigilant lors d'un paiement sur Internet
11. Séparer les usages personnels des usages professionnels
12. Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

Pour aller plus loin 1

Découvrir la CyberSécurité

Guide des bonnes pratiques de l’informatique ANSSI

Bienvenue sur le MOOC de l'ANSSI

Pour aller plus loin 2

Suivre l’actualité de la CyberSécurité
www.cybermalveillance.gouv.fr

Guide des bonnes pratiques de l’informatique de l’ANSSI

Bienvenue sur le MOOC de l'ANSSI

E-sensibilisation en ligne & Veille

https://www.cybermalveillance.gouv.fr/mon-espace/apprendre

- Mieux connaître les menaces cyber actuelles
- Vous approprier les bonnes pratiques
- Comprendre l'intérêt et la manière de transmettre ces réflexes et sensibiliser à votre tour

Exemple de CyberAttaques

free

HARVEST

PARIS 2024

FFTA
Fédération Française de Tir à l'Arc

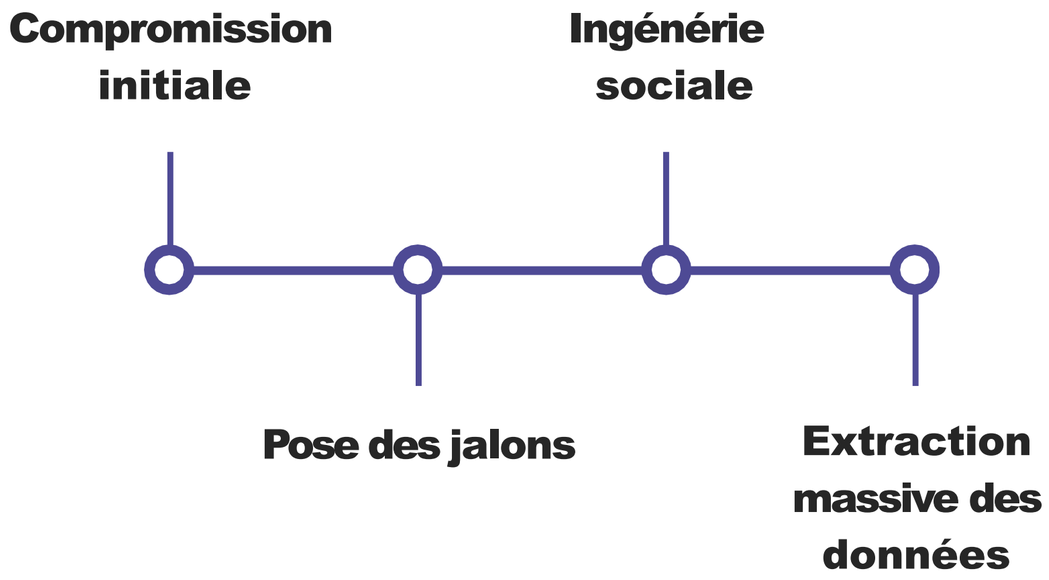
free

Octobre 2024

Vol de DCP de **19,2 millions** de clients dont **5,11 millions de coordonnées bancaires**

Base de données mise en vente pour **20.000€**

Mineur de 17 ans arrêté le 15 janvier 2025
Mise en place un numéro vert



Source : CyberMalveillance.gouv.fr

PARIS 2024

Juillet/Août 2024

43 manœuvres informationnelles contre les J.O. 2024

Attaques DDoS contre les infrastructures durant la cérémonie d'ouverture.

Doxxing athlètes : Faire du doxxing, c'est divulguer publiquement sur internet des informations personnelles (souvent privées ou sensibles) sur quelqu'un sans son consentement, dans le but de le nuire, de le harceler ou de l'intimider.

Création de contenu de désinformation durant les jeux.

HARVEST

Février 2025

Harvest, une entreprise française spécialisée dans la création de logiciels pour la gestion de patrimoine et les services financiers, a été victime d'un cyber-incident.

L'attaque est survenue via un serveur hébergé chez un prestataire de Harvest. Le groupe de pirates a revendiqué l'attaque et publié des données volées.

Ce qu'il s'est passé : Des données clients appartenant à des banques privées, des assureurs et des conseillers en gestion de patrimoine ont été compromises. Les logiciels de Harvest ont dû être suspendus, ce qui a perturbé les clients de l'entreprise.

Leçons à retenir pour une PME : Le point d'entrée n'était pas la PME directement, mais un prestataire/serveur externe - Highlight : la chaîne d'approvisionnement est une faiblesse !

Même une entreprise spécialisée (logiciels métiers) peut subir un arrêt d'activité ou une perte de données qui impacte fortement ses clients - pour une PME, cela peut être critique.

Importance de prévoir : sauvegardes, continuité d'activité, plans de réponse.

Janvier 2025

La Fédération Française de Tir à l'Arc a constaté **qu'environ 77 256 de ses licenciés avaient été avertis d'un accès frauduleux à leurs données** via un prestataire. Les données exposées incluaient noms, prénoms, dates de naissance, adresses mail/postales, photos de profil. Les mots de passe restaient chiffrés et non compromis.

Ce qu'il s'est passé : Une faille de sécurité chez un prestataire chargé des espaces licences/dirigeants pour plusieurs fédérations a été exploitée. Les licenciés ont été informés, et des mesures de réinitialisation d'accès ont été annoncées.

Leçons à retenir pour une PME : Même dans une structure "non commerciale" (association/fédération), les données personnelles sont ciblées - donc vos données clients, collaborateurs sont aussi à protéger.

Le point de vulnérabilité : prestataire/tiers - encore une fois, le maillon externe est une porte d'entrée fréquente. Même si les mots de passe n'ont pas été compromis, la fuite des données "moins sensibles" peut entraîner perte de confiance et coûts de communication.

Exemple de désinformation 1

Une étude révèle que 47 % des Français affirment avoir déjà été confrontés à une **fakenews** en santé et que 43 % ont déjà pris une décision basée sur une information fausse.

Vidéo à propos de **Brigitte Macron**

Opération de désinformation russe « Storm-15-16 » ciblant la France

Fake-news ciblant les Forces armées françaises dans le contexte ukrainien

Ministère des Armées / armée : Le ministère a publié un « décryptage » d'une fausse information ciblant les forces armées françaises. Il s'agissait de messages sur les réseaux sociaux accusant les militaires d'être envoyés dans un conflit semblable à la Première Guerre mondiale ou incitant à « refuser les ordres », avec un objectif de démoralisation ou division.

Exemple de désinformation 2

Climat / médias français : Un rapport d'ONG a recensé **128 « intox »** sur le climat dans les médias audiovisuels français pendant 3 mois, de janvier à aout 2025, 529 affirmations erronées sur le climat ont été relevées dans les médias français.

Santé / accès à l'information : Le Ministère de la Santé a organisé un colloque en avril 2025 (« Lutte contre l'obscurantisme et la désinformation en santé ») pour aborder l'ampleur des fausses informations dans le domaine de la santé.

Politique / influence étrangère : Le ministère des Armées rappelle que la désinformation est « une arme de guerre », utilisée par certains États (notamment cités la Russie) pour influencer l'opinion publique française et internationale.

Un cas précis : une vidéo virale montrait Emmanuel Macron (et d'autres dirigeants européens) et un objet blanc dans un train vers Kiev - certains ont prétendu qu'il s'agissait de cocaïne, ce que la France a dénoncé comme fake news diffusée par des ennemis.

Exemples concrets d'arnaques IA

Anne, une femme française de 53 ans, a été victime d'une escroquerie où un individu se faisant passer pour l'acteur Brad Pitt lui a soutiré 830 000 € …

---

1. Appel ou visio pour ordonner un virement important (deepfake)
2. Usurpation vocale d'un proche pour demander de l'argent
3. Phishing ultra-personnalisé généré par IA
4. Faux entretiens d'embauche / avatars IA pour voler documents
5. Publicité *deepfake* pour arnaques crypto ou achats frauduleux

Une deepfake est un contenu - souvent une vidéo, une image, ou une voix - fabriqué ou modifié par une intelligence artificielle pour imiter une personne réelle de façon très réaliste.

Comment ça fonctionne : L'IA apprend à partir de centaines d'images, vidéos ou enregistrements vocaux d'une personne (trouvés en ligne, sur les réseaux, dans des vidéos publiques…). Etc.

Signes d’alerte
ce qui doit vous faire hésiter

L’urgence absolue (pression pour agir dans l’heure).

Demande de transfert vers un compte inconnu, crypto, ou recharge de cartes cadeau.

La personne refuse un **appel retour** ou une vérification via un autre canal (SMS, e-mail pro, message signé).

Discrépances audio/vidéo : lèvres mal synchronisées, voix « *métallique* », arrière-plan flou, ou qualité trop « *parfaite* ».

Lien/QRCode qui ne correspond pas au nom de la société (URL raccourcie suspecte).

Requêtes d’envoi de documents sensibles pour un « *entretien* » non sollicité.

Le coût des cyberattaques explose en France

Estimation du coût annuel de la cybercriminalité en France, en milliards de dollars américains