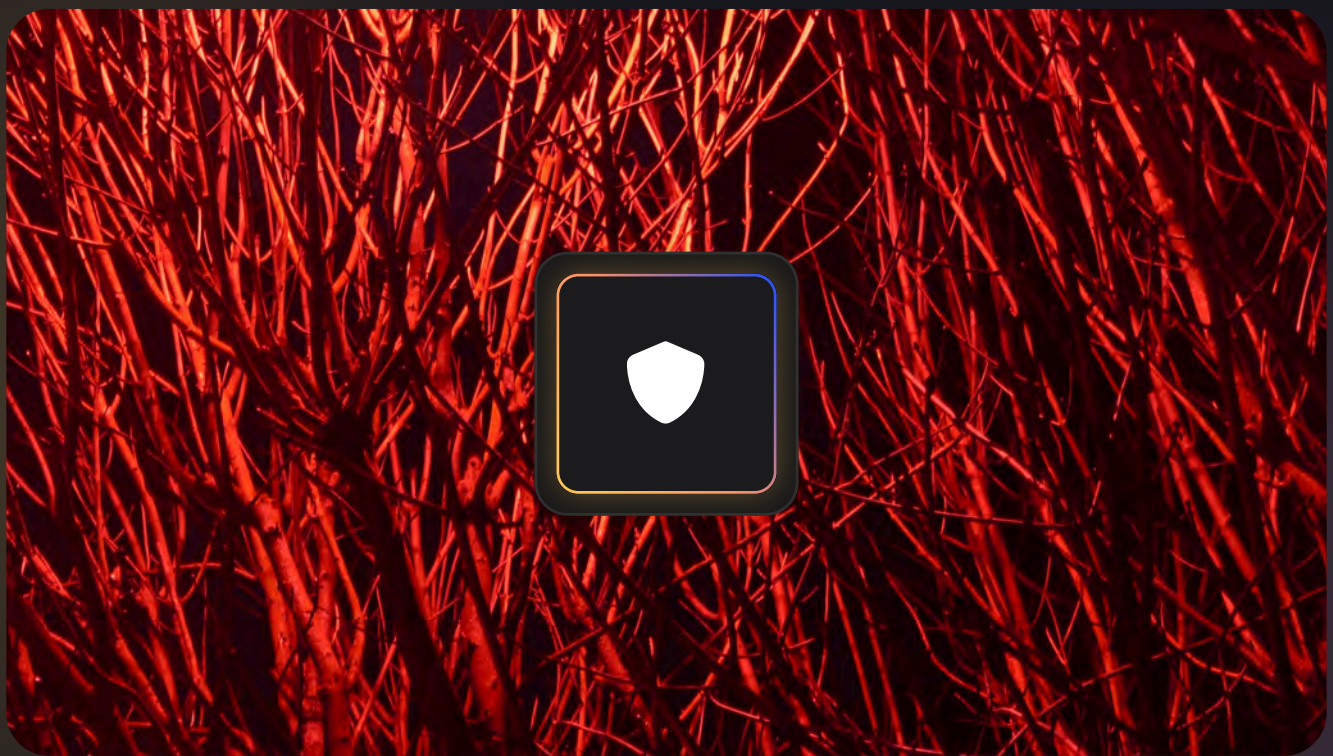
LIVRE BLANC

# 15 menaces cyber en entreprise

## Comment s'en protéger ?



MAILINBLACK

# Contexte

Dans un monde de plus en plus numérique et interconnecté, la cybersécurité est devenue un **enjeu majeur** pour les entreprises de toutes tailles et de tous secteurs. Chaque jour, **des millions de cyberattaques** sont lancées à travers le globe, menaçant :

- la confidentialité
- l'intégrité
- la disponibilité des données

Face à cette réalité, il est fondamental de **comprendre les risques encourus** et de **mettre en place des stratégies efficaces** pour protéger les informations sensibles et assurer la continuité des activités.

Les cyberattaques ne ciblent pas uniquement les grandes multinationales. **Les petites et moyennes entreprises** (PME), souvent moins bien préparées, sont particulièrement **vulnérables**. Une simple attaque peut avoir des conséquences dramatiques :

- arrêt temporaire de la production
- atteinte à la réputation de l'entreprise
- perte de données clients
- sanctions légales (si les données personnelles sont mal protégées)

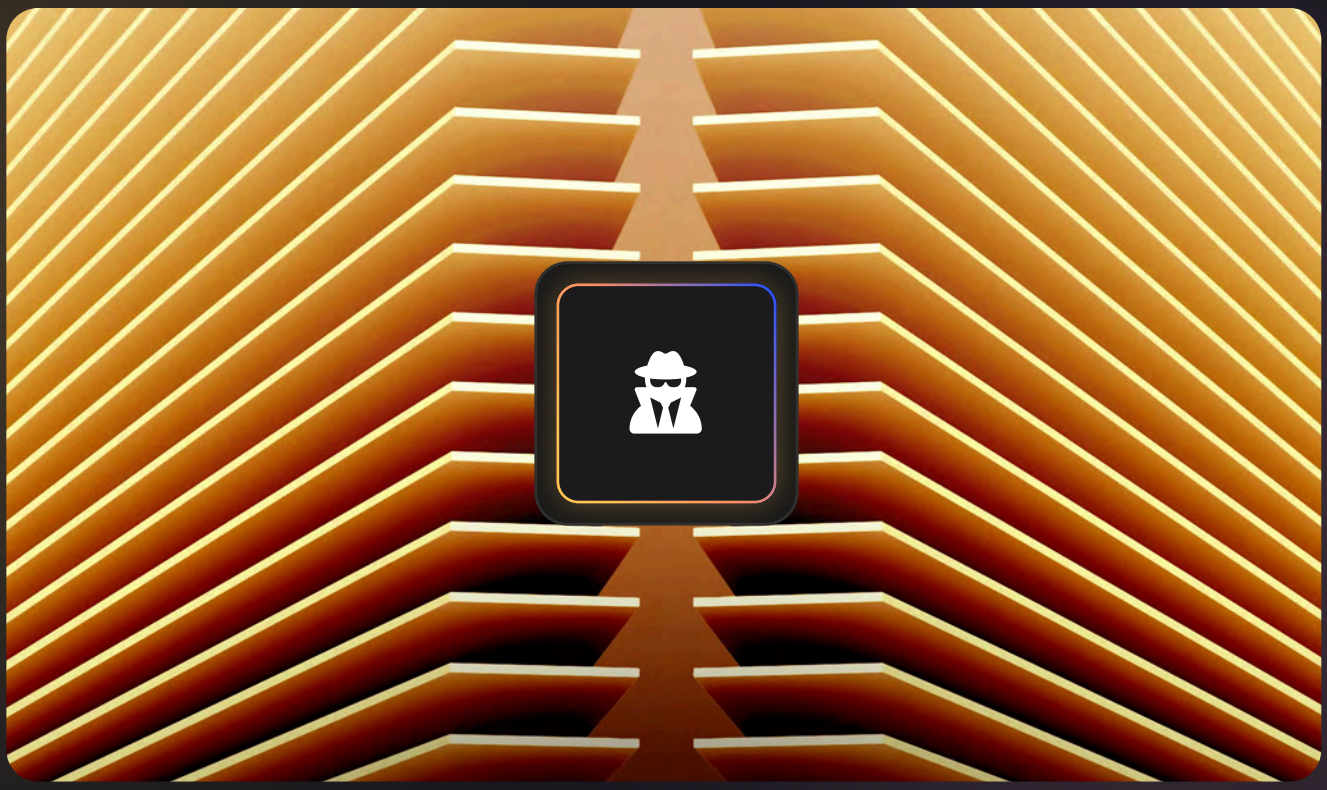
Les motivations derrière ces attaques sont variées. Certaines visent à obtenir des **informations confidentielles à des fins de chantage** ou de **revente sur le marché noir**. D'autres cherchent à **déstabiliser une entreprise** pour des raisons concurrentielles ou idéologiques. Il existe également des cybercriminels qui exploitent des failles de sécurité simplement pour le **plaisir de causer des dommages**.

Ce livre blanc a pour objectif de vous **fournir une vision claire et détaillée des menaces les plus courantes** auxquelles les entreprises sont confrontées aujourd'hui. En comprenant les risques et en adoptant des outils de protection adaptés, vous serez mieux armés pour faire face à l'évolution constante des menaces numériques. La cybersécurité n'est pas une simple question technique : **c'est une démarche globale qui concerne l'ensemble des collaborateurs et qui requiert une vigilance permanente**.

# Sommaire

1

# Qu’est-ce qu’un hackeur ?



Le terme "hackeur" suscite souvent des images de personnes encapuchonnées tapant frénétiquement sur des claviers dans des pièces sombres. Mais en réalité, le concept de hackeur est bien plus complexe et nuancé. Un hackeur est une personne qui possède des compétences techniques avancées en informatique et qui utilise ces compétences pour comprendre, modifier ou exploiter les systèmes informatiques. Cependant, l'utilisation qu'il fait de ses compétences dépend de ses motivations et de son éthique.

Le mot "hackeur" trouve ses origines dans les années 1960 au MIT (Massachusetts Institute of Technology). À cette époque, le terme était utilisé pour désigner des programmeurs passionnés qui cherchaient à optimiser les performances des ordinateurs et à repousser les limites techniques. Il s'agissait alors d'une communauté de bidouilleurs éthiques cherchant à comprendre les systèmes en profondeur.

Avec l'arrivée d'Internet et la numérisation massive des informations, l'hacking a évolué. De nouveaux acteurs sont apparus, exploitant les failles de sécurité à des fins malveillantes. Aujourd'hui, l'hacking est une pratique qui peut être légale ou illégale, constructive ou destructrice.

# Types de hackeurs

Il est important de distinguer les différents types de hackeurs en fonction de leurs motivations et de leur éthique. Voici les principaux types :

### White Hats
*(hackeurs éthiques)*

Les White Hats sont des hackeurs éthiques qui utilisent leurs compétences pour renforcer la sécurité des systèmes d'information.

Leur objectif principal est d'identifier et de corriger les vulnérabilités avant qu'elles ne soient exploitées par des individus malveillants. Ils agissent toujours avec l'autorisation des entreprises et respectent un cadre légal et éthique strict.

### Exemples d'activités

- **Tests d'intrusion (pentests) :** simulation contrôlée d'attaques pour évaluer les défenses d'un système et détecter les failles de sécurité.
- **Audits de sécurité :** analyse approfondie des politiques de sécurité en place pour proposer des améliorations adaptées.
- **Bug bounty** : participation à des programmes de récompense où les hackeurs éthiques signalent des failles en échange d'une compensation financière.

### Exemple

SaxX, **Clément Domingo** de son vrai nom, est un spécialiste de la cybercriminalité.

Il a notamment fondé l'ONG hackeurs Without Borders, pour former et sensibiliser à ce sujet.

## Black Hats
*(hackeurs malveillants)*

Les Black Hats exploitent les vulnérabilités des systèmes informatiques pour des motifs illégaux tels que le vol de données, l'extorsion ou le sabotage. Ils opèrent sans autorisation et peuvent causer d'importants dommages financiers et réputationnels aux entreprises.

### Exemples d'activités

- **Attaques par ransomware :** blocage des systèmes avec demande de rançon pour restaurer l'accès
- **Vol de données sensibles :** exploitation des failles pour dérober des informations confidentielles
- **Phishing :** campagnes de faux emails pour obtenir des identifiants ou des informations bancaires

### Exemple

L'attaque de **WannaCry** en 2017 a affecté des centaines de milliers d'ordinateurs à travers le monde.

## Gray Hats
*(hackeurs ambigus)*

Les Gray Hats naviguent entre l'éthique des White Hats et les actions illégales des Black Hats. Ils repèrent des vulnérabilités sans autorisation, mais ne les exploitent pas nécessairement à des fins malveillantes. Ils peuvent signaler les failles aux entreprises, parfois contre rémunération, sans avoir été mandatés pour le faire.

### Exemples d'activités

- **Détection non sollicitée de failles :** identifier et divulguer des vulnérabilités découvertes par hasard
- **Proposition de correctifs :** offrir leurs services après avoir signalé une faille

### Exemple

**Marcus Hutchins**, également connu sous le pseudonyme MalwareTech, est reconnu pour son rôle dans l'arrêt de l'attaque mondiale du ransomware WannaCry en 2017.

## Script Kiddies
*(hackeurs ambigus)*

Les Script Kiddies sont des individus peu expérimentés qui utilisent des outils préexistants pour lancer des attaques, souvent sans en comprendre le fonctionnement en profondeur. Leur objectif est généralement le vandalisme ou le gain de reconnaissance.

### Exemples d'activités

- **DDoS (déni de service distribué) :** saturer un site pour le rendre inaccessible.
- **Utilisation de malwares** téléchargeables : exploiter des kits de piratage en ligne.

### Exemple

Des **adolescents** menant des attaques contre des serveurs de jeux en ligne pour perturber les sessions de joueurs.

## Hacktivistes

Les hacktivistes utilisent l'hacking pour promouvoir des causes politiques, sociales ou idéologiques. Leurs attaques visent à sensibiliser le public ou à protester contre certaines pratiques.

### Exemples d'activités

- **Défiguration de sites web :** remplacement du contenu par des messages politiques.
- **Divulgation de données sensibles :** fuites d'informations pour dénoncer des injustices.

### Exemple

Le collectif Anonymous a mené des opérations contre des sites gouvernementaux pour protester contre des lois liberticides.

## State-Sponsored *(hackeurs d'État)*

Ces hackeurs sont financés ou soutenus par des gouvernements pour mener des opérations de cyberespionnage, de sabotage ou de propagande contre d'autres nations.

### Exemples d'activités

- **Espionnage industriel :** vol de secrets commerciaux d'entreprises étrangères.
- **Sabotage d'infrastructures critiques :** attaques contre les réseaux énergétiques ou de transport.

### Exemple

Le groupe APT28 (Fancy Bear), lié à la Russie, a été impliqué dans plusieurs attaques contre des cibles politiques et militaires.


## Blue Hats

Les Blue Hats sont souvent des consultants externes engagés pour tester la sécurité d'un système avant son déploiement. Leur objectif est de s'assurer qu'aucune vulnérabilité majeure ne subsiste.

### Exemples d'activités

- **Vérification finale de sécurité avant lancement :** tests préliminaires pour détecter des failles restantes.
- **Simulations d'attaques spécifiques :** focus sur des scénarios particuliers de menace.

### Exemple

Des **experts sollicités** avant la mise en ligne d'une nouvelle application bancaire.

## Red Team

La Red Team désigne une équipe de hackeurs professionnels chargée de simuler des attaques réalistes contre une organisation pour tester ses défenses. Ils utilisent des tactiques offensives complexes pour évaluer l'efficacité des mécanismes de sécurité.

### Exemples d'activités

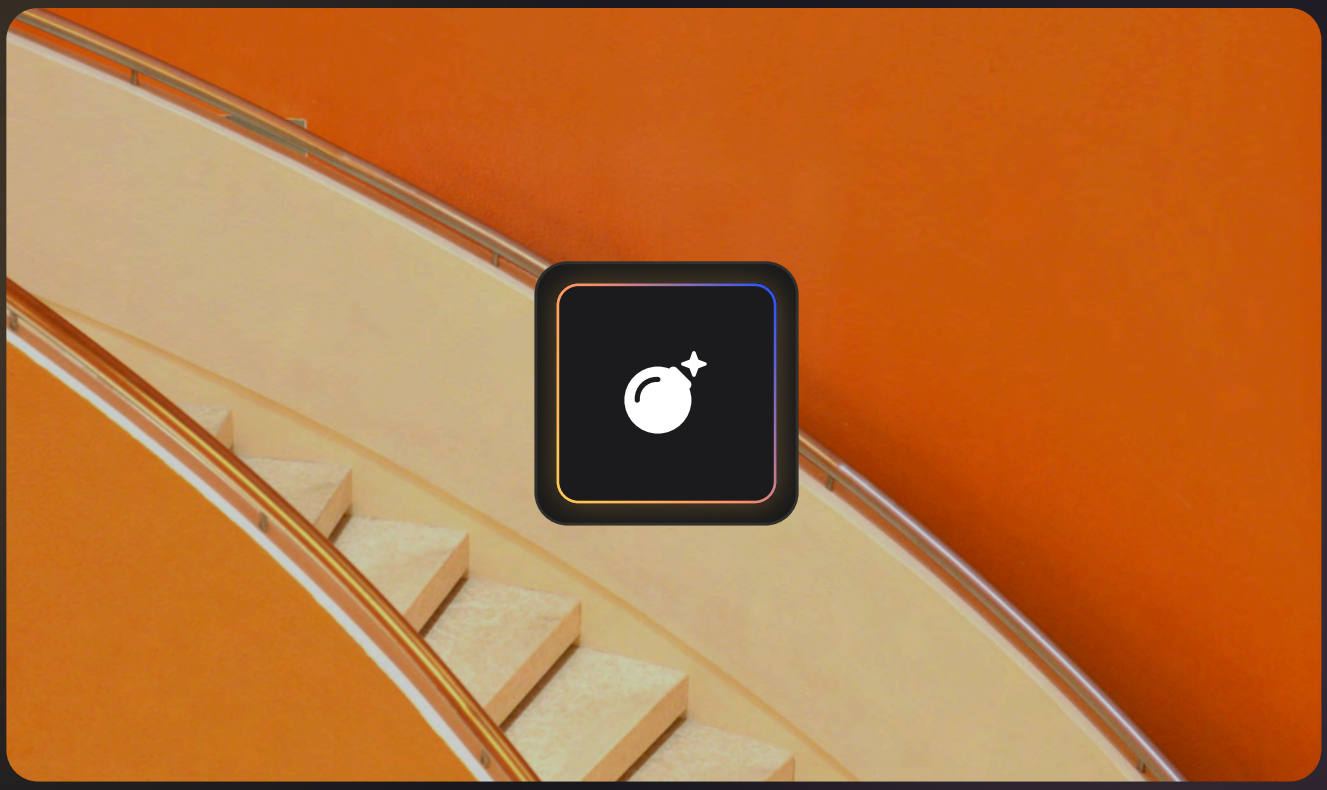
- **Scénarios d'attaques avancées :** test des capacités de détection et de réponse des équipes internes.
- **Exploitation de failles humaines :** ingénierie sociale pour contourner les mesures de sécurité.

### Exemple

Une **Red Team mandatée** pour tester la sécurité physique et numérique d'une entreprise financière.

2

# TOP 15
# des menaces rencontrées dans les entreprises



# 1. Ransomware

**+53%**

**d'attaques par ransomware**
en France en 2024 selon l'ANSSI

**+10 milliards d'€**

de pertes financières liées aux ransomwares par an en Europe

Les ransomwares sont aujourd'hui l'une des menaces les plus coûteuses pour les entreprises. Selon l'ANSSI, les attaques par ransomware ont augmenté de 53% en 2024 en France. Le groupe LockBit a revendiqué 13 attaques rien qu'au deuxième trimestre 2024, tandis que des groupes comme BlackCat (ALPHV), 8Base, Royal, Clop, et RansomHub continuent de sévir à travers le pays.
Les pertes financières liées aux ransomwares dépassent les 10 milliards d'euros par an en Europe, avec des secteurs critiques très ciblés comme :

- la santé
- les collectivités
- l'industrie

## Qu'est-ce que c'est ?

Un ransomware (ou rançongiciel) est un logiciel malveillant qui **chiffre les fichiers d'une organisation** et **exige une rançon** pour fournir la clé de déchiffrement. Les attaques modernes combinent souvent le chiffrement des données avec le vol d'informations sensibles, une technique appelée double extorsion. Cela permet aux attaquants d'ajouter une pression supplémentaire en menaçant de publier ou vendre ces données si la rançon n'est pas payée.

## Comment ça fonctionne ?

1. **Infection initiale**
   Les attaquants utilisent des méthodes variées pour infiltrer les systèmes : emails de phishing avec pièces jointes infectées, failles de sécurité non corrigées dans les systèmes ou services distants, téléchargements malveillants sur des sites compromis.
2. **Chiffrement**
   Une fois infiltré, le ransomware chiffre les fichiers et systèmes de l'entreprise, rendant les données inaccessibles.
3. **Demande de rançon**
   Une note exige le paiement d'une rançon (généralement en cryptomonnaie) en échange de la clé de déchiffrement.
4. **Double extorsion**
   Les attaquants volent les données avant de les chiffrer et menacent de les divulguer si la rançon n'est pas payée.

## Comment s'en protéger ?

**Sauvegarder régulièrement les données** et conserver des copies déconnectées du réseau.

**Mettre à jour les systèmes et logiciels** avec les derniers correctifs de sécurité.

**Filtrer les emails entrants** pour bloquer les pièces jointes et liens malveillants.

**Restreindre et sécuriser les accès distants** avec une authentification multifacteurs (MFA).

**Segmenter le réseau** pour limiter la propagation en cas d'attaque.

**Former les employés** aux bonnes pratiques de cybersécurité pour éviter les erreurs humaines.

# 2. Phishing

**90%**

des violations de sécurité sont **des attaques de phishing**

**84%**

des organisations françaises ont été **victimes d'au moins une tentative de phishing** en 2023

Le phishing est l'une des attaques les plus fréquentes et les plus efficaces contre les entreprises. En 2023, près de 84% des organisations françaises ont été victimes d'au moins une tentative de phishing, selon le baromètre de la cybersécurité de CESIN. Les attaques de phishing représentent environ 90% des violations de sécurité, ce qui en fait une menace omniprésente et redoutable pour les entreprises.

## Qu'est-ce que c'est ?

Le phishing (ou hameçonnage) est une technique de fraude par laquelle un attaquant **se fait passer pour une entité de confiance** (banque, administration, fournisseur de services) afin de tromper la victime et **lui soutirer des informations sensibles** comme des identifiants, des mots de passe ou des informations bancaires. Le phishing se déroule le plus souvent par email, mais il peut aussi prendre la forme de SMS (smishing) ou d'appels téléphoniques (vishing).

# Comment ça fonctionne ?

1. **Création du leurre**
   L'attaquant conçoit un email frauduleux imitant une entreprise ou une organisation légitime. L'email contient souvent un message d'urgence ou une incitation à agir rapidement (par exemple : "Votre compte sera désactivé sous 24h").

2. **Envoi de l'email**
   L'email est envoyé en masse à une liste de victimes potentielles. Le message contient un lien ou une pièce jointe malveillante.

3. **Redirection vers un faux site**
   Si la victime clique sur le lien, elle est dirigée vers un faux site qui ressemble à s'y méprendre au site officiel (par exemple : une fausse page de connexion bancaire).

4. **Collecte des informations**
   La victime entre ses informations personnelles (identifiants, mots de passe, etc.) sur le faux site. Ces données sont alors récupérées par l'attaquant.

5. **Exploitation des données**
   L'attaquant utilise ces informations pour accéder aux comptes de la victime, effectuer des transactions frauduleuses ou vendre les données sur le dark web.

# Comment s'en protéger ?

**Analyser les emails suspects :**
- Vérifier l'adresse de l'expéditeur.
- Rechercher les erreurs de grammaire ou d'orthographe inhabituelles.
- Être vigilant face aux demandes urgentes ou aux offres trop alléchantes.

**Ne pas cliquer sur les liens douteux :**
- Passer le curseur sur le lien pour afficher l'URL réelle avant de cliquer.
- Accéder aux sites officiels en tapant directement l'URL dans le navigateur.

**Utiliser des solutions de filtrage anti-phishing :** déployer des solutions de sécurité des emails pour bloquer les tentatives de phishing en amont.

**Activer l'authentification multifacteurs (MFA) :** ajouter une couche de sécurité supplémentaire pour protéger les comptes même si les identifiants sont compromis.

**Former régulièrement les employés :**
- Organiser des simulations de phishing pour sensibiliser les équipes.
- Proposer des modules d'e-learning sur la détection des attaques par phishing.

# 3. Spearphishing

**+231%**

**d'attaques de spearphishing** en 2024

Notre Baromètre Cyber 2025 nous a permis de réaliser, qu'en 2024, les attaques de spearphishing ont augmenté de +231% par rapport à l'année précédente. Pourquoi ? Parce que de nouvelles formes de spearphishing se développent :

**Whaling :** usurpation d'identité de hauts dirigeants pour accéder à des données sensibles ou détourner des fonds.

**Usurpation de fils de conversation :** les attaquants se glissent dans des échanges d'emails légitimes via des boîtes compromises, insérant des liens ou fichiers malveillants pour exploiter la confiance contextuelle.

**IA génératives :** elle permet aux hackeurs d'améliorer leurs tactiques d'ingénierie sociale, rendant les attaques plus sophistiquées et difficiles à détecter.

## Qu'est-ce que c'est ?

Le spearphishing est une forme avancée de phishing où l'attaquant **cible une personne ou une organisation spécifique avec des emails personnalisés**. Contrairement au phishing traditionnel, qui envoie des messages en masse, le spearphishing utilise des informations précises sur la victime (poste, collègues, projets en cours) pour rendre l'attaque crédible. L'objectif est souvent d'obtenir des identifiants, des informations confidentielles ou d'installer des logiciels malveillants.

## Comment ça fonctionne ?

1. **Collecte d'informations**
   L'attaquant recherche des informations détaillées sur la cible à partir des réseaux sociaux, sites professionnels ou fuites de données.
2. **Création du message**
   Un email personnalisé est conçu pour imiter une source de confiance (collègue, supérieur hiérarchique, fournisseur). Le message contient souvent une pièce jointe malveillante ou un lien vers un faux site.
3. **Interaction de la victime**
   La victime, croyant le message authentique, clique sur le lien ou ouvre la pièce jointe, ce qui peut permettre le vol d'informations ou l'installation d'un malware.
4. **Exploitation**
   L'attaquant utilise les informations volées pour accéder aux systèmes, voler des données ou exécuter des fraudes financières.

## Comment s'en protéger ?

**Sensibilisation et formation continue :**
- Former régulièrement les employés à détecter les signes de spearphishing.
- Utiliser des simulations pour renforcer les réflexes face à des attaques ciblées.

**Vérification systématique des demandes :**
- Confirmer les demandes inhabituelles par un autre canal (appel téléphonique ou message direct).
- Examiner attentivement les adresses email et les liens.

**Implémenter des solutions de sécurité avancées :**
- Utiliser des filtres anti-phishing pour bloquer les emails suspects.
- Mettre en place une authentification multifacteurs (MFA) pour sécuriser les comptes.

**Réduire la visibilité des informations sensibles :** limiter les informations professionnelles disponibles en ligne (organigrammes, projets en cours).

**Surveillance et détection :** analyser les communications pour identifier rapidement des activités suspectes.

# 4. Spam

**7,3 milliards**

**d'envois de spam par jour** ciblant la France

**+293%**

d'attaques par email le premier semestre 2024, par rapport à la même période en 2023

La France est le deuxième pays le plus ciblé par les hackeurs, avec pas moins de 7,3 milliards de spams reçus par jour. À l'échelle mondiale, environ 3,4 milliards de spams inondent quotidiennement les boîtes de réception. Selon Acronis, le premier semestre 2024 a vu une augmentation stupéfiante de 293% des attaques par email par rapport à la même période en 2023. Si le spam est souvent perçu comme une simple nuisance, il constitue en réalité un vecteur majeur pour des attaques plus graves telles que :

- le phishing
- les ransomwares
- l'installation de malwares

## Qu’est-ce que c’est ?

Le spam désigne l’**envoi massif et non sollicité d’emails**, souvent à des fins publicitaires, mais aussi pour diffuser des contenus malveillants. Les spams peuvent inclure :

- Des publicités frauduleuses (produits miracles, services douteux).
- Des liens malveillants redirigeant vers des sites infectés.
- Des tentatives de phishing se faisant passer pour des entités légitimes.
- Des pièces jointes infectées déployant des logiciels malveillants.

## Comment ça fonctionne ?

1. **Collecte d’adresses email**
   Les spammeurs utilisent des robots pour récupérer des adresses sur le web, achètent des bases de données compromises, ou exploitent des formulaires en ligne mal sécurisés.
2. **Envoi massif**
   Les spams sont diffusés à grande échelle via des serveurs compromis ou des botnets pour éviter d’être détectés par les systèmes de sécurité.
3. **Leurres et incitations**
   Les messages contiennent des offres trop belles pour être vraies, des alertes urgentes ou des incitations à agir rapidement pour tromper les destinataires.
4. **Action malveillante**
   En cliquant sur les liens ou en ouvrant les pièces jointes, les utilisateurs peuvent être redirigés vers des sites frauduleux, télécharger des malwares, ou divulguer des informations sensibles.

## Comment s’en protéger ?

**Utiliser des filtres anti-spam avancés :** déployer des solutions capables de bloquer les spams avant qu’ils n’atteignent les boîtes de réception.

**Éviter de publier son adresse email publiquement :** limiter le partage d’adresses sur des sites ou forums non sécurisés.

**Ne pas ouvrir d’emails suspects :** se méfier des expéditeurs inconnus et des messages non sollicités avec des objets trop accrocheurs.

**Ne pas cliquer sur des liens douteux :** survoler les liens pour vérifier l’URL avant de cliquer.

**Utiliser des adresses email temporaires** : pour les inscriptions sur des sites peu fiables, privilégier des adresses jetables.

**Former les employés :** sensibiliser les équipes aux risques liés aux spams et aux bonnes pratiques pour éviter les infections.

# 5. DDoS (Déni de Service Distribué)

**+111%**

**d'attaques DDoS** pour le premier semestre 2024 vs 2023

**8,5 millions**

d'attaques DDoS au cours des six premiers mois de l'année

Selon le rapport d'Imperva sur les cybermenaces pour le premier semestre 2024, le nombre d'attaques DDoS a explosé, enregistrant une hausse de 111% au premier semestre par rapport à la même période en 2023. Cloudflare a atténué 8,5 millions d'attaques DDoS au cours des six premiers mois de l'année, avec 4,5 millions au premier trimestre et 4 millions au deuxième trimestre.

Des événements politiques et sociaux ont également déclenché des vagues d'attaques : par exemple, après l'entrée de la Suède dans l'OTAN, les attaques DDoS contre le pays ont été multipliées par cinq, une tendance similaire à celle observée lors de l'adhésion de la Finlande en 2023. En Europe, l'arrestation de Pavel Durov, fondateur de Telegram, a déclenché une série d'attaques ciblant des sites français et européens.

## Qu'est-ce que c'est ?

Une attaque par Déni de Service Distribué (DDoS) vise à **rendre un site web, un service en ligne ou une infrastructure réseau indisponible** en le saturant de requêtes simultanées. Les attaquants utilisent des botnets — des réseaux d'appareils compromis — pour générer un trafic massif. Ces attaques peuvent provoquer des interruptions de service, des pertes financières considérables et nuire à la réputation des organisations visées.

## Types d'attaques DDoS

**Attaques par volume**

Saturent la bande passante du réseau avec un trafic massif.

**Attaques par protocole**

Exploitent des vulnérabilités dans les protocoles réseau (ex. : SYN Flood).

**Attaques applicatives**

Visent les failles spécifiques des applications web pour épuiser leurs ressources.

# Comment ça fonctionne ?

1. **Infection des appareils**
   Les attaquants créent un botnet en infectant des ordinateurs, serveurs, et appareils IoT (objets connectés).
2. **Coordination de l'attaque**
   Les appareils compromis sont activés simultanément pour envoyer un nombre massif de requêtes vers la cible.
3. **Surcharge du système**
   Le serveur ou le réseau ciblé devient incapable de traiter le volume de requêtes, ce qui entraîne une interruption du service.
4. **Impact sur les services**
   Les utilisateurs légitimes ne peuvent plus accéder au site ou au service concerné, ce qui peut durer des heures, voire des jours.

# Comment s'en protéger ?

**Solutions de mitigation DDoS :** utiliser des services spécialisés pour absorber et filtrer le trafic malveillant avant qu'il n'atteigne le réseau cible (par exemple : services Cloudflare).

**Surveillance et détection proactive :** mettre en place des systèmes de monitoring réseau pour détecter rapidement des pics de trafic anormaux.

**Augmentation de la capacité réseau :** élargir la bande passante pour absorber les pics de trafic lors d'une attaque volumineuse

**Pare-feux et systèmes de prévention d'intrusion (IPS) :** configurer des pare-feux et des systèmes IPS pour bloquer les requêtes suspectes avant qu'elles n'atteignent le serveur.

**Utiliser des CDN (Réseaux de Distribution de Contenu) :** répartir le trafic via un CDN pour éviter les points de saturation uniques.

**Plan de réponse aux incidents :** établir un plan de continuité d'activité pour minimiser l'impact en cas d'attaque et assurer une reprise rapide des services.

# 6. Ingénierie Sociale

**81%**

des entreprises constate une **augmentation des tentatives d'hameçonnage**

**150 jours**

pour se remettre d'une violation de données pour 35% des entreprises

En 2024, 81% des entreprises ont constaté une augmentation des tentatives d'hameçonnage. De plus, 3 utilisateurs sur 4 ne sont pas conscients des techniques d'ingénierie sociale, rendant ces attaques particulièrement efficaces. Les conséquences peuvent être graves : 35% des entreprises victimes mettent plus de 150 jours à se remettre d'une violation de données et seules 12% déclarent s'être totalement rétablies après une attaque selon IMB. Exploitant la faiblesse humaine, ces attaques continuent d'être une menace majeure pour la sécurité des entreprises.

## Qu'est-ce que c'est ?

L'ingénierie sociale consiste à **manipuler psychologiquement des individus pour leur soutirer des informations confidentielles** ou les inciter à réaliser des actions compromettantes. Plutôt que d'exploiter des failles techniques, ces attaques ciblent le facteur humain.

### Formes d'attaques d'ingénierie social :

**Phishing**

Emails frauduleux incitant à divulguer des informations.

**Pretexting**

Création de scénarios fictifs pour obtenir des données.

**Baiting**

Proposer des appâts (clés USB infectées, téléchargements gratuits).

**Vishing**

Appels téléphoniques frauduleux pour extorquer des informations.

**Quid Pro Quo**

Promettre une récompense en échange d'informations.

# Comment ça fonctionne ?

1. **Collecte d'informations**
   Les attaquants recueillent des données sur la cible (poste, collègues, habitudes) via les réseaux sociaux, sites professionnels ou fuites de données.

2. **Élaboration du scénario**
   Un scénario crédible est créé pour gagner la confiance de la cible (par exemple, un faux appel du service IT demandant des identifiants).

3. **Interaction et manipulation**
   La victime reçoit un message ou un appel personnalisé. Le ton est souvent pressant ou rassurant pour inciter à l'action.

4. **Exploitation des informations**
   Les données obtenues sont utilisées pour accéder aux systèmes, lancer des attaques ou commettre des fraudes.

# Comment s'en protéger ?

**Former les employés régulièrement :**
- Sensibiliser aux différentes formes d'ingénierie sociale avec des simulations et des ateliers.
- Intégrer des scénarios réalistes pour tester leur vigilance.

**Mettre en place des procédures de vérification :** vérifier l'authenticité des demandes d'informations sensibles via un canal indépendant (appel direct, message personnel).

**Limiter les informations publiques :** réduire les informations disponibles sur les employés et projets sur les réseaux sociaux et sites web.

**Adopter des politiques de sécurité strictes :** établir des protocoles pour les transferts de fonds et l'accès aux données sensibles.

**Implémenter l'authentification multifacteurs (MFA) :** ajouter une couche de sécurité pour protéger les comptes contre l'accès non autorisé.

# 7. Malware

**36%**

des techniques d'attaque recensées sont **des malwares**

En 2024, les cyberattaques impliquant des logiciels malveillants ont atteint des niveaux sans précédent, illustrant une menace croissante pour les entreprises et les institutions à travers le monde. Selon Hackmegon, les logiciels malveillants, ou malwares, ont constitué 36% des techniques d'attaque recensées, en hausse par rapport aux 35% de l'année précédente.

## Qu'est-ce que c'est ?

Le terme malware (contraction de malicious software) englobe tous les **types de logiciels malveillants conçus pour nuire aux systèmes informatiques**.

### Types de malwares les plus courants :

**Virus**

Se reproduisent en infectant d'autres fichiers.

**Chevaux de Troie**

Se font passer pour des logiciels légitimes tout en exécutant des actions malveillantes en arrière-plan.

**Vers (Worms)**

Se propagent automatique--ment via les réseaux.

**Spyware**

Espionnent les activités des utilisateurs pour voler des informations sensibles.

**Ransomware**

Chiffrent les données et exigent une rançon pour les déverrouiller.

## Comment ça fonctionne ?

1. **Infection initiale**
   Le malware est diffusé via des emails malveillants avec des pièces jointes infectées, des téléchargements depuis des sites compromis (drive-by downloads), des supports amovibles comme des clés USB infectées et des failles de sécurité non corrigées dans les logiciels et systèmes.
2. **Exécution du malware**
   Une fois ouvert ou téléchargé, le malware s'installe sur le système.
3. **Propagation**
   Certains malwares se propagent automatiquement à travers le réseau pour infecter d'autres appareils.
4. **Actions malveillantes**
   Vol de données personnelles et professionnelles, espionnage des activités des utilisateurs et sabotage des fichiers et des systèmes.

## Comment s'en protéger ?

**Utiliser des solutions de sécurité à jour :** installer des antivirus et anti-malwares avec des bases de signatures régulièrement mises à jour.

**Filtrer les emails entrants :** déployer des solutions anti-spam et anti-phishing pour bloquer les emails suspects avant qu'ils n'atteignent les utilisateurs.

**Maintenir les systèmes à jour :** appliquer les correctifs de sécurité pour combler les failles exploitables.

**Limiter l'usage des périphériques externes :** contrôler et restreindre l'utilisation de supports amovibles non sécurisés.

**Former les employés :** sensibiliser les équipes à identifier les emails suspects et les sites potentiellement dangereux.

**Segmenter le réseau :** diviser le réseau en segments pour limiter la propagation en cas d'infection.

# 9. Rogue Software (Logiciel Faussement Légitime)

**450 000**

**nouveaux malwares étaient détectés chaque jour** en 2023

**92%**

des logiciels malveillants sont distribués par emai

En 2023, plus de 450 000 nouveaux malwares étaient détectés chaque jour, selon AV-TEST. Parmi ces menaces, les rogue software représentent une catégorie particulièrement insidieuse. Ils se font passer pour des logiciels légitimes, notamment des solutions de sécurité ou d'optimisation du système, mais leur véritable objectif est d'infecter les systèmes pour dérober des informations ou installer d'autres malwares. Environ 92 % des logiciels malveillants sont distribués par email, ce qui en fait le vecteur principal pour ces faux logiciels.

## Qu'est-ce que c'est ?

Un rogue software (ou logiciel frauduleux) est un **programme malveillant déguisé en application légitime**.

Ces logiciels frauduleux affichent souvent de fausses alertes pour inciter l'utilisateur à :

- Payer une version complète pour supprimer des menaces inexistantes.
- Installer des malwares supplémentaires en arrière-plan.
- Divulguer des informations personnelles comme des identifiants ou des informations bancaires

## Un rogue software peut-être déguisé en :

**Un antivirus gratuit**

Proposant de scanner et nettoyer votre système.

**Un optimiseur de performance**

Promettant d'accélérer le système ou de libérer de l'espace disque.

**Une fausse mise à jour logicielle**

Incitant à télécharger une prétendue mise à jour de sécurité.

## Comment ça fonctionne ?

1. **Leurre publicitaire ou pop-up**
   L'utilisateur voit une publicité ou une alerte indiquant une infection ou un problème système urgent.
2. **Téléchargement et installation**
   Croyant résoudre un problème, l'utilisateur télécharge et installe le logiciel frauduleux.
3. **Fausses analyses et alertes**
   Le logiciel effectue une analyse fictive et affiche des menaces inexistantes pour créer un sentiment d'urgence.
4. **Demande de paiement ou d'action**
   L'utilisateur est invité à acheter une version complète ou à cliquer sur des liens malveillants.
5. **Infection et exploitation**
   Le logiciel installe des malwares, vole des informations ou compromet le système.

## Comment s'en protéger ?

**Utiliser des logiciels de sécurité reconnus :** télécharger uniquement des antivirus et logiciels depuis les sites officiels des éditeurs.

**Éviter les popups et alertes suspectes :**

- Ne pas cliquer sur des publicités ou alertes indiquant des infections inattendues.
- Utiliser le gestionnaire de tâches pour fermer une fenêtre suspecte.

**Maintenir les systèmes à jour :** installer régulièrement les correctifs de sécurité pour éviter les vulnérabilités exploitées par ces logiciels frauduleux.

**Installer des bloqueurs de publicités :** utiliser des extensions de navigateur pour bloquer les publicités malveillantes et réduire le risque d'exposition.

**Former les employés :** sensibiliser aux signes des rogue software et aux pratiques sûres de téléchargement.

**Analyser les logiciels avant installation :** utiliser des outils de sécurité pour analyser les fichiers téléchargés avant de les exécuter.

# 10. Man-in-the-Middle (MitM)

**19%**

**des cyberattaques réussies** sont de type Man-in-the-Middle

**300 jours**

c'est le temps moyen qu'une entreprise met pour détecter l'attaque de MitM

En 2024, les attaques de type Man-in-the-Middle (MitM) représentent environ 19% de toutes les cyberattaques réussies, selon plusieurs rapports sur la cybersécurité. Avec la généralisation des connexions via Wi-Fi publics, les appareils mobiles et les réseaux professionnels sont de plus en plus vulnérables. Ces attaques peuvent prendre en moyenne 300 jours avant d'être détectées, comme l'indique le rapport d'IBM X-Force et du Ponemon Institute. Les cybercriminels exploitent ces failles pour intercepter des données sensibles telles que des identifiants de connexion ou des informations financières.

## Qu'est-ce que c'est ?

Une attaque Man-in-the-Middle (MitM) consiste à **intercepter et, parfois, à altérer les communications entre deux parties à leur insu**. L'attaquant se place « au milieu » pour espionner, collecter des informations confidentielles, ou rediriger la victime vers des sites frauduleux. Ces attaques sont particulièrement courantes sur les réseaux Wi-Fi publics non sécurisés.

## Exemples d'attaques :

**Wi-Fi publics compromis**

L'attaquant crée un faux point d'accès pour capturer le trafic des utilisateurs.

**Usurpation DNS ou IP**

Redirection vers des sites malveillants pour voler des identifiants.

**Interception SSL/TLS**

Exploitation de failles pour déchiffrer les communications sécurisées.

# Comment ça fonctionne ?

1. **Intrusion dans le réseau**
   L'attaquant se connecte au même réseau que la cible, souvent en utilisant un Wi-Fi public compromis ou un faux hotspot.
2. **Interception des communications**
   L'attaquant utilise des outils spécialisés pour capturer le trafic échangé entre la victime et le serveur légitime.
3. **Modification ou redirection**
   L'attaquant peut espionner les informations échangées (identifiants, mots de passe) et altérer les messages pour injecter du code malveillant ou rediriger vers des sites frauduleux.
4. **Exploitation des données**
   Les informations volées sont utilisées pour accéder aux comptes de la victime, effectuer des fraudes financières ou lancer d'autres attaques.

# Comment s'en protéger ?

**Utiliser des connexions sécurisées :**
- Éviter d'utiliser des Wi-Fi publics pour des opérations sensibles.
- Utiliser un VPN (Réseau Privé Virtuel) pour chiffrer le trafic.

**Vérifier les certificats SSL/TLS :**
- S'assurer que les sites web utilisent HTTPS.
- Ne jamais ignorer les avertissements de sécurité du navigateur concernant les certificats.

**Mettre à jour régulièrement les systèmes :** appliquer les correctifs de sécurité pour combler les vulnérabilités exploitées par les attaquants.

**Activer l'authentification multifacteurs (MFA) :** ajouter une couche de sécurité supplémentaire pour protéger les comptes même en cas de compromission des identifiants.

**Sensibiliser les utilisateurs :** former les employés aux risques des connexions non sécurisées et aux bonnes pratiques de cybersécurité.

**Surveiller les activités réseau :** utiliser des solutions de détection d'intrusion (IDS) pour repérer les comportements suspects sur le réseau.

# 11. Credential Stuffing

**60%**

des tentative d'attaques **sont du Credential Stuffing** dans le monde en 2024

**1,5 milliard**

de tentatives de Credential Stuffing dans le monde chaque jour

Les attaques par Credential Stuffing représentent une menace croissante pour les entreprises et les utilisateurs. En 2024, environ 60% des attaques contre les entreprises impliquent une tentative de Credential Stuffing, selon Akamai. Chaque jour, on dénombre près de 1,5 milliard de tentatives de Credential Stuffing dans le monde. Cette menace exploite la mauvaise habitude de 65% des utilisateurs qui réutilisent le même mot de passe sur plusieurs comptes (Google). L'automatisation et la disponibilité des identifiants volés sur le dark web rendent ces attaques particulièrement efficaces.

## Qu'est-ce que c'est ?

Le Credential Stuffing consiste à **utiliser des combinaisons d'identifiants** (emails, noms d'utilisateur, mots de passe) **récupérés lors de fuites de données pour tenter de se connecter à différents services en ligne**. Les cybercriminels misent sur la réutilisation fréquente des mots de passe par les utilisateurs pour accéder frauduleusement à leurs comptes.

## Comment ça fonctionne ?

1. **Collecte des identifiants volés**
   Les attaquants obtiennent des listes d'identifiants via des fuites de données ou en les achetant sur le dark web.
2. **Automatisation des tentatives de connexion**
   Des bots testent automatiquement des milliers de combinaisons d'identifiants sur de multiples sites web.
3. **Accès aux comptes compromis**
   Une fois les identifiants valides trouvés, les attaquants peuvent :
   - Voler des informations sensibles.
   - Effectuer des achats frauduleux.
   - Prendre le contrôle de comptes pour lancer d'autres attaques.

## Comment s'en protéger ?

**Utiliser des mots de passe uniques et complexes :**
- Éviter la réutilisation des mots de passe sur plusieurs comptes.
- Opter pour des phrases de passe longues et difficiles à deviner.

**Activer l'authentification multifacteurs (MFA) :** ajouter une vérification supplémentaire pour sécuriser les comptes.

**Utiliser un gestionnaire de mots de passe :** faciliter la création et la gestion de mots de passe uniques pour chaque service.

**Surveiller les connexions suspectes :** mettre en place des systèmes d'alerte pour détecter les activités inhabituelles.

**Notifier après des tentatives de connexion échouées :** informer les utilisateurs en cas de tentatives de connexion suspectes.

**Vérifier si vos identifiants ont été compromis :** utiliser des services comme Have I Been Pwned pour vérifier l'exposition de vos identifiants.

# 12. Zero-Day Exploits

**+56%**

**de failles Zero-Day ont été exploitées** en 2023 par rapport en 2022

Les Zero-Day Exploits sont des vulnérabilités de sécurité qui sont exploitées avant que les éditeurs de logiciels n'aient eu le temps de les corriger. En 2023, 97 failles Zero-Day ont été exploitées, marquant une augmentation de 56% par rapport à 2022, selon un rapport de Mandiant. Ces exploits ciblent principalement les systèmes Windows (43% des attaques) et les navigateurs web (36%). Ces attaques représentent une menace particulièrement grave, car elles sont utilisées avant qu'un correctif ne soit disponible, permettant aux attaquants de compromettre des systèmes en toute discrétion.

### Qu'est-ce que c'est ?

Un Zero-Day Exploit désigne une **faille dans un logiciel ou un système pour laquelle il n'existe pas encore de correctif**, souvent car elle est inconnue des développeurs. L'attaquant découvre la vulnérabilité et l'exploite avant même que la société qui a créé le logiciel ne soit au courant et n'ait eu le temps de déployer une mise à jour de sécurité.

EXEMPLE

En janvier 2024, une vulnérabilité Zero-Day a été exploitée dans Microsoft Exchange. L'attaque a permis à des cybercriminels d'exécuter du code à distance sur les serveurs Exchange vulnérables, compromettant les données sensibles de milliers d'organisations dans le monde entier avant qu'un patch de sécurité ne soit mis en place. Cette exploitation a exposé des failles critiques dans les systèmes de messagerie d'entreprises et d'administrations publiques.

## Comment ça fonctionne ?

1. **Découverte de la vulnérabilité**
   L'attaquant identifie une faille de sécurité dans un logiciel ou un système d'exploitation.
2. **Création et développement de l'exploit**
   L'attaquant développe un code malveillant pour exploiter cette faille avant qu'un patch ne soit publié.
3. **Lancement de l'attaque**
   L'exploit est utilisé pour pénétrer un système cible souvent de manière furtive.
4. **Exploitation continue**
   Les attaquants peuvent voler des données, installer des malwares ou étendre leur accès au réseau.

## Comment s'en protéger ?

**Maintenir les systèmes à jour :** appliquer les mises à jour de sécurité dès leur publication pour combler les vulnérabilités connues.

**Surveiller les alertes de sécurité :** s'abonner aux bulletins de sécurité pour recevoir des informations immédiates sur les vulnérabilités et les correctifs.

**Utiliser des solutions de sécurité avancées :** déployer des systèmes de détection des intrusions (IDS) et des technologies de réponse aux points de terminaison (EDR) pour identifier les comportements suspects.

**Mettre en place une défense multicouche :** combiner des pare-feux, des antivirus et des solutions de filtrage de contenu pour protéger les systèmes contre les failles Zero-Day.

**Segmenter le réseau :** diviser le réseau pour limiter l'impact d'une attaque exploitant une faille Zero-Day.

**Former les employés :** sensibiliser les équipes aux bonnes pratiques de cybersécurité et à la gestion des risques liés aux exploits Zero-Day.

# 13. Attaques sur les Objets Connectés (IoT)

**10 milliards**

**d'appareils connectés en 2023**

En 2024, les attaques ciblant les objets connectés (IoT) ont considérablement augmenté, reflétant une montée des cybermenaces envers ces appareils. Selon un rapport de Zscaler, les cyberattaques visant les dispositifs IoT et OT continuent de croître, en partie en raison de leur prolifération rapide et de leur sécurité souvent insuffisante. Avec plus de 10 milliards d'appareils connectés en 2023, de nombreux dispositifs présentent des vulnérabilités exploitables. Ces failles en font des cibles privilégiées pour les cybercriminels, qui les utilisent pour infiltrer des réseaux, exfiltrer des données sensibles ou constituer des botnets. Une étude de l'ANSSI met également en lumière l'importance de renforcer les mesures de sécurité dans un contexte où les tensions géopolitiques amplifient les risques.

## Qu'est-ce que c'est ?

Les objets connectés (IoT) sont des **dispositifs physiques qui se connectent à Internet pour collecter, échanger ou recevoir des données**. Ces appareils incluent des caméras de sécurité, des thermostats intelligents, des dispositifs médicaux connectés, des ampoules intelligentes, et bien d'autres encore. Cependant, leur faible niveau de sécurité, souvent dû à des mises à jour logicielles négligées ou à une configuration de sécurité insuffisante, les rend vulnérables aux attaques.

EXEMPLE

En 2023, une attaque DDoS massive a utilisé des appareils IoT compromis pour perturber plusieurs services en ligne dans le monde entier. Des caméras de sécurité et des routeurs domestiques ont été infiltrés, permettant aux cybercriminels de lancer l'attaque à partir de milliers d'appareils infectés. Cette attaque a montré la capacité des hackeurs à transformer des objets connectés vulnérables en armes pour paralyser des réseaux.

# Comment ça fonctionne ?

1. **Infiltration des appareils IoT**
   Les cybercriminels exploitent des vulnérabilités dans les appareils IoT pour y accéder à distance. Cela peut inclure des failles dans les logiciels ou des défauts de configuration.

2. **Prise de contrôle**
   Une fois l'appareil compromis, l'attaquant peut en prendre le contrôle pour l'utiliser comme point d'entrée dans un réseau plus large.

3. **Exploitation et exfiltration**
   L'attaquant peut voler des données sensibles, espionner les utilisateurs, ou utiliser les appareils IoT pour des attaques DDoS en envoyant un trafic massif vers des cibles externes.

4. **Propagation de l'attaque**
   Les objets IoT compromis peuvent être utilisés pour attaquer d'autres appareils ou étendre l'accès à d'autres parties du réseau.

# Comment s'en protéger ?

**Sécuriser les appareils IoT :**
- Assurez-vous que les appareils IoT sont configurés avec des mots de passe forts et uniques.
- Changez les mots de passe par défaut.

**Mettre à jour régulièrement les logiciels :** appliquez les mises à jour de sécurité pour corriger les vulnérabilités dans les appareils IoT.

**Segmenter le réseau :** isolez les appareils IoT du réseau principal de l'entreprise afin de limiter l'impact en cas de compromission.

**Utiliser des solutions de sécurité adaptées :** déployer des firewalls et des systèmes de détection d'intrusion (IDS) pour protéger le réseau des appareils IoT.

**Auditer régulièrement la sécurité des appareils IoT :** effectuer des audits de sécurité pour identifier les faiblesses dans les dispositifs IoT.

**Former les utilisateurs :** sensibiliser les employés à la sécurité des objets connectés et à la configuration correcte de ces dispositifs.

# 14. Attaques par Force Brute

**80%**

des violations de données sont **liées à des identifiants compromis en 2024**

**5%**

des violations de données sont des attaques par force brute

Les attaques par force brute représentent environ 5% des violations de données et sont responsables de nombreuses intrusions dans des systèmes mal sécurisés. En 2024, 80% des violations de données sont liées à des identifiants compromis, avec une part significative de ces attaques réalisées par force brute. Ces attaques sont courantes dans les systèmes utilisant des mots de passe faibles ou réutilisés. Par exemple, une étude menée par Malwarebytes a montré que les attaques par force brute sont particulièrement efficaces contre les systèmes de gestion de contenu et les services en ligne utilisant des mots de passe simples.

## Qu'est-ce que c'est ?

Une attaque par force brute consiste à **tester systématiquement toutes les combinaisons possibles de mots de passe ou de clés de chiffrement jusqu'à ce que la bonne soit trouvée**. Ces attaques sont automatisées et peuvent durer plusieurs heures ou jours selon la complexité du mot de passe, ce qui les rend particulièrement efficaces contre des mots de passe faibles.

## Comment ça fonctionne ?

1. **Identification de la cible**
   L'attaquant sélectionne un compte ou un système à cibler.
2. **Collecte d'informations**
   Récupération de noms d'utilisateur ou d'adresses e-mail associés au compte cible.
3. **Lancement de l'attaque**
   Utilisation d'outils automatisés pour tester différentes combinaisons de mots de passe.
4. **Accès obtenu**
   Une fois le mot de passe correct trouvé, l'attaquant accède au compte ou au système.

## Comment s'en protéger ?

**Utiliser des mots de passe forts et uniques :** combiner lettres majuscules et minuscules, chiffres et caractères spéciaux.

**Mettre en place l'authentification multifacteurs (MFA) :** ajouter une couche de sécurité supplémentaire.

**Limiter les tentatives de connexion :** bloquer temporairement un compte après plusieurs tentatives échouées.

**Surveiller les activités suspectes :** mettre en place des alertes pour détecter des tentatives de connexion inhabituelles.

# 15. Attaques de la Chaîne d'Approvisionnement

**+40%**

**d'attaques de la chaîne d'approvisionnement en 2024**

**18 000**

organisations dans le monde affecté par l'attaque de la chaîne d'approvisionnement en 2023

Les attaques de la chaîne d'approvisionnement ont fortement augmenté en 2024, représentant environ 40% des attaques ciblant des entreprises. Selon Symantec, près de 60% des entreprises ont été touchées par des attaques utilisant des vulnérabilités dans la chaîne d'approvisionnement. Ces attaques visent souvent les fournisseurs de services ou de logiciels tiers pour pénétrer dans les systèmes d'une organisation cible. En 2023, l'attaque de la chaîne d'approvisionnement sur SolarWinds a affecté plus de 18 000 organisations dans le monde, y compris des agences gouvernementales et des entreprises privées, après qu'un logiciel mis à jour a été compromis pour distribuer des malwares.

## Qu'est-ce que c'est ?

Les attaques de la chaîne d'approvisionnement se produisent lorsque des cybercriminels **exploitent des vulnérabilités dans les systèmes d'un fournisseur tiers, dans le but d'atteindre leur véritable cible**. Ces attaques peuvent se produire à n'importe quel point de la chaîne d'approvisionnement, que ce soit chez un fournisseur de logiciels, de matériel ou même un prestataire de services cloud. Les attaquants visent souvent des entreprises ayant des relations étroites avec leurs victimes, en cherchant à exploiter des failles dans les logiciels ou les processus de gestion des données.

## Comment ça fonctionne ?

1. **Identification de la cible indirecte**
   Les attaquants ciblent un fournisseur de services ou un partenaire de l'entreprise.
2. **Exploitation de la vulnérabilité**
   Une fois la vulnérabilité identifiée, l'attaquant l'exploite pour pénétrer dans les systèmes du fournisseur et injecter des malwares.
3. **Propagation de l'attaque**
   L'attaquant utilise l'accès au fournisseur pour propager l'attaque aux organisations clientes ou partenaires de ce fournisseur.
4. **Exploitation des données**
   L'attaquant vole des informations sensibles, effectue des attaques DDoS ou infiltre des réseaux internes pour un espionnage ou un sabotage.

## Comment s'en protéger ?

**Auditer les fournisseurs et partenaires :** effectuer des évaluations régulières de la sécurité des fournisseurs et partenaires pour identifier les vulnérabilités potentielles.

**Mettre en œuvre une sécurité des logiciels tiers :** vérifier l'intégrité des mises à jour logicielles et des outils fournis par les tiers avant leur déploiement.

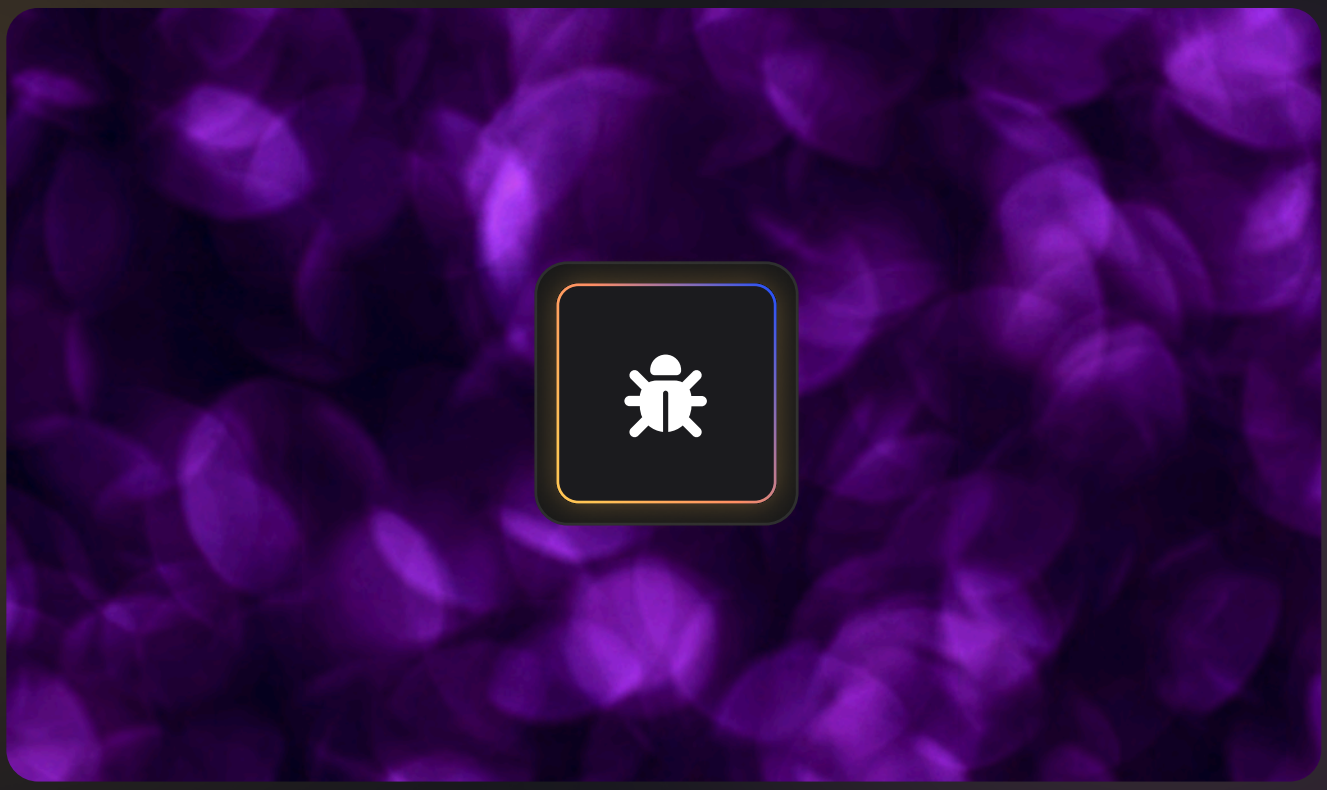
**Sensibiliser les équipes à la gestion des risques :** former les équipes à reconnaître les menaces provenant des fournisseurs et à suivre les meilleures pratiques pour la gestion des risques de la chaîne d'approvisionnement.

**Mettre en place une réponse rapide :** avoir un plan de réponse aux incidents spécifique aux attaques de la chaîne d'approvisionnement, incluant la communication rapide et l'isolation des systèmes compromis.

**Renforcer la sécurité des systèmes internes :** segmenter les réseaux pour limiter les possibilités d'attaque si un fournisseur tiers est compromis.

3

# TOP 10
# **des attaques récentes majeures en france**



Les cyberattaques en France en 2024 ont affecté de nombreux secteurs, allant des infrastructures critiques à des entreprises privées. Voici un aperçu des dix principales cyberattaques, leurs impacts et les leçons à en tirer.

# 1. Hôpital Simone Veil de Cannes

HÔPITAL DE CANNES SIMONE VEIL

- Janvier 2024
- Rasnomware
- Paralysie du SI

Le Centre Hospitalier Simone Veil de Cannes a été frappé en janvier 2024 par une attaque par ransomware, paralysant les systèmes informatiques de l'hôpital. Les données des patients ont été chiffrées, rendant les dossiers médicaux inaccessibles. L'attaque a également perturbé la gestion des urgences et des soins. Le personnel a dû recourir à des registres papier pour suivre les traitements. Après l'attaque, une enquête a révélé que les cybercriminels avaient réussi à infiltrer le réseau hospitalier via une vulnérabilité non corrigée dans un logiciel tiers utilisé par l'hôpital.

LEÇON

La cybersécurité dans les institutions de santé nécessite une attention particulière, surtout pour les logiciels tiers utilisés pour la gestion des données sensibles.

# 2. Groupe Ramsay Santé

Ramsay Santé

- Janvier 2024
- Paralysie des serveurs gérant les infrastructures et les messageries

Le groupe Ramsay Santé, qui possède 120 établissements de santé en France, a été victime d'une cyberattaque le 25 janvier 2024. Cette attaque a paralysé les serveurs gérant les infrastructures et les messageries du groupe, obligeant tout le personnel à revenir aux méthodes manuelles, en utilisant du stylo et du papier pour gérer les dossiers des patients et les communications. Cette situation de crise a perturbé les soins aux patients et a duré une semaine. Le virus responsable de cette attaque a été décrit comme particulièrement destructeur, affectant de nombreux systèmes internes de gestion.

En réponse, Ramsay Santé a travaillé avec l'ANSSI pour sécuriser ses systèmes et restaurer les services, mais les opérations ont été perturbées pendant plusieurs jours.

LEÇON

Cette cyberattaque met en lumière la vulnérabilité des établissements de santé, qui dépendent souvent de systèmes informatiques complexes pour gérer les soins et les données des patients. Il est indispensable pour les établissements médicaux de renforcer leurs mesures de cybersécurité et d'être préparés à des attaques potentielles, en particulier celles utilisant des ransomwares.

## 3. SNCF

- Janvier 2024
- Désorganisation des services ferroviaires

Fin janvier 2024, La SNCF a été victime d'une cyberattaque qui a perturbé ses services de réservation en ligne et sa gestion des horaires en 2024. Les attaquants ont exploité des vulnérabilités dans les systèmes de gestion des données de transport pour désorganiser les services ferroviaires. L'attaque a causé des retards importants, affectant des milliers de passagers.

LEÇON

Les entreprises de transport doivent renforcer la sécurité de leurs systèmes de gestion des horaires et de billetterie, qui sont des cibles de choix pour les cybercriminels.

Ces attaques montrent que, quels que soient les secteurs, les cybercriminels cherchent de plus en plus à exploiter des vulnérabilités dans les entreprises et les administrations françaises. Elles soulignent la nécessité de renforcer les mesures de cybersécurité pour protéger les infrastructures critiques et les données sensibles.

## 4. Société Générale

- Janvier 2024
- Phishing et Credential stuffing
- Transactions frauduleuses

En début d'année 2024, Société Générale, une grande banque française, a été ciblée par une attaque par phishing suivie d'une tentative de credential stuffing. Les attaquants ont utilisé des identifiants obtenus illégalement pour accéder à des comptes bancaires et effectuer des transactions frauduleuses. La banque a rapidement détecté l'intrusion et a bloqué les comptes compromis.

LEÇON

Les banques doivent mettre en place des solutions d'authentification forte et des alertes en temps réel pour détecter toute activité suspecte.

# 5. France Travail

France Travail

- Février 2024
- Phishing et logiciels malveillants
- Accès à des infos personnelles sensibles

En février 2024, France Travail, l'agence nationale pour l'emploi et les services publics, a été victime d'une cyberattaque majeure, ciblant sa plateforme de gestion des dossiers de demandeurs d'emploi. Les attaquants ont infiltré les systèmes et ont eu accès à des informations personnelles sensibles. Les autorités ont suspendu l'accès aux services en ligne pendant plusieurs jours pour contenir l'attaque et évaluer les dommages. Le groupe de hackeurs a utilisé une combinaison de phishing et de logiciels malveillants pour s'introduire dans le réseau.

LEÇON

Cette attaque souligne la nécessité de protéger les bases de données personnelles et de renforcer la sécurité des plateformes publiques traitant des informations sensibles.

# 6. Saint-Nazaire

SAINT-NAZAIRE

- Avril 2024
- Logiciels malveillants
- Perturbation des services publics

La ville de Saint-Nazaire, dans le département de la Loire-Atlantique, a été victime d'une cyberattaque en avril 2024. L'attaque a ciblé l'infrastructure municipale, perturbant les services publics tels que la gestion des déchets, l'éclairage public et l'administration des transports locaux. Les cybercriminels ont utilisé des logiciels malveillants pour infiltrer le système informatique de la municipalité. La ville a dû recourir à des méthodes de gestion manuelle pour assurer la continuité des services pendant la crise.

LEÇON

Les administrations locales doivent renforcer la sécurité de leurs systèmes pour éviter de telles perturbations, qui peuvent affecter les services essentiels.

# 7. Engie

- Mai 2024
- Exploitation des vulnérabilités dans des logiciels tiers
- Perturbations des opérations

Le groupe énergétique Engie a été ciblé en mai 2024 par une cyberattaque qui a affecté son infrastructure informatique. L'attaque a perturbé les opérations de plusieurs centrales électriques, bien que le groupe ait affirmé qu'il n'y avait pas de risques pour la fourniture d'énergie. Les hackeurs ont réussi à pénétrer le réseau de l'entreprise en exploitant des vulnérabilités dans des logiciels tiers utilisés pour la gestion des systèmes industriels.

LEÇON

Cette attaque rappelle la vulnérabilité des infrastructures critiques et l'importance d'une surveillance constante des systèmes industriels.

# 8. Jeux Olympiques de Paris 2024

- 2024
- DDoS
- Tentative d'nfiltration des systèmes

Les Jeux Olympiques de Paris 2024 ont été la cible de plusieurs tentatives de cyberattaques en raison de l'ampleur de l'événement. Bien que les autorités françaises aient déployé des mesures de sécurité renforcées pour protéger les infrastructures critiques, des hackeurs ont tenté d'infiltrer les systèmes pour perturber les événements. Une attaque par DDoS (Déni de service distribué) a été déjouée avant qu'elle n'affecte les plateformes en ligne et les systèmes de billetterie.

LEÇON

Les administrations locales doivent renforcer la sécurité de leurs systèmes pour éviter de telles perturbations, qui peuvent affecter les services essentiels.

# 9. Intersport


- 2024
- Ransomware
- Perturbations dans les opérations

Intersport, un détaillant d'articles de sport, a subi une attaque de type ransomware en 2024. L'attaque a affecté la plateforme de vente en ligne et la gestion des stocks, entraînant des perturbations dans les opérations. Les données sensibles des clients, y compris les informations de paiement, ont été compromises.

LEÇON

Les entreprises de détail doivent renforcer leur cybersécurité, notamment pour leurs plateformes d'e-commerce, et se préparer à répondre aux attaques de ransomwares.

# 10. Attaque de Free


- Novembre 2024
- Ransomware
- Pannes de service

En novembre 2024, Free, fournisseur majeur d'accès à Internet, a été victime d'une cyberattaque qui a perturbé une partie de son réseau pendant plusieurs jours. Cette attaque a ciblé les infrastructures de gestion des abonnés, ce qui a causé des pannes de service pour des milliers d'utilisateurs à travers la France. Les cybercriminels ont utilisé un ransomware sophistiqué pour verrouiller l'accès aux bases de données des abonnés et ont exigé une rançon en échange de la clé de déchiffrement. Free a réagi en mettant en place un plan d'urgence pour restaurer les services et renforcer ses mesures de sécurité.

LEÇON

Cette attaque rappelle l'importance de sécuriser les bases de données sensibles et de préparer un plan de continuité d'activité face aux ransomwares.

4

# Comment U-Cyber 360° peut aider les entreprises à réduire les risques humains ?

Dans un contexte où les cybermenaces sont omniprésentes, les entreprises doivent impérativement adopter des solutions proactives pour se protéger avant qu'une attaque ne survienne. U-Cyber 360° de Mailinblack propose une approche globale de la cybersécurité qui s'intègre parfaitement aux besoins des organisations face à des menaces de plus en plus sophistiquées.

## Protection contre le phishing et les ransomwares

Comme l'ont montré les attaques sur Ramsay Santé ou Société Générale, la sécurité des emails est essentielle. Les solutions Mailinblack filtrent les emails malveillants, bloquant ainsi les tentatives de phishing et de ransomware avant qu'elles n'atteignent les collaborateurs.

## Préparation aux attaques ciblées

Pour les entreprises confrontées à des menaces de spearhishing, les solutions Mailinblack offrent une protection avancée qui permet de détecter et de prévenir les attaques plus ciblées, réduisant ainsi le risque de compromission des informations sensibles.

## Gestion des mots de passe

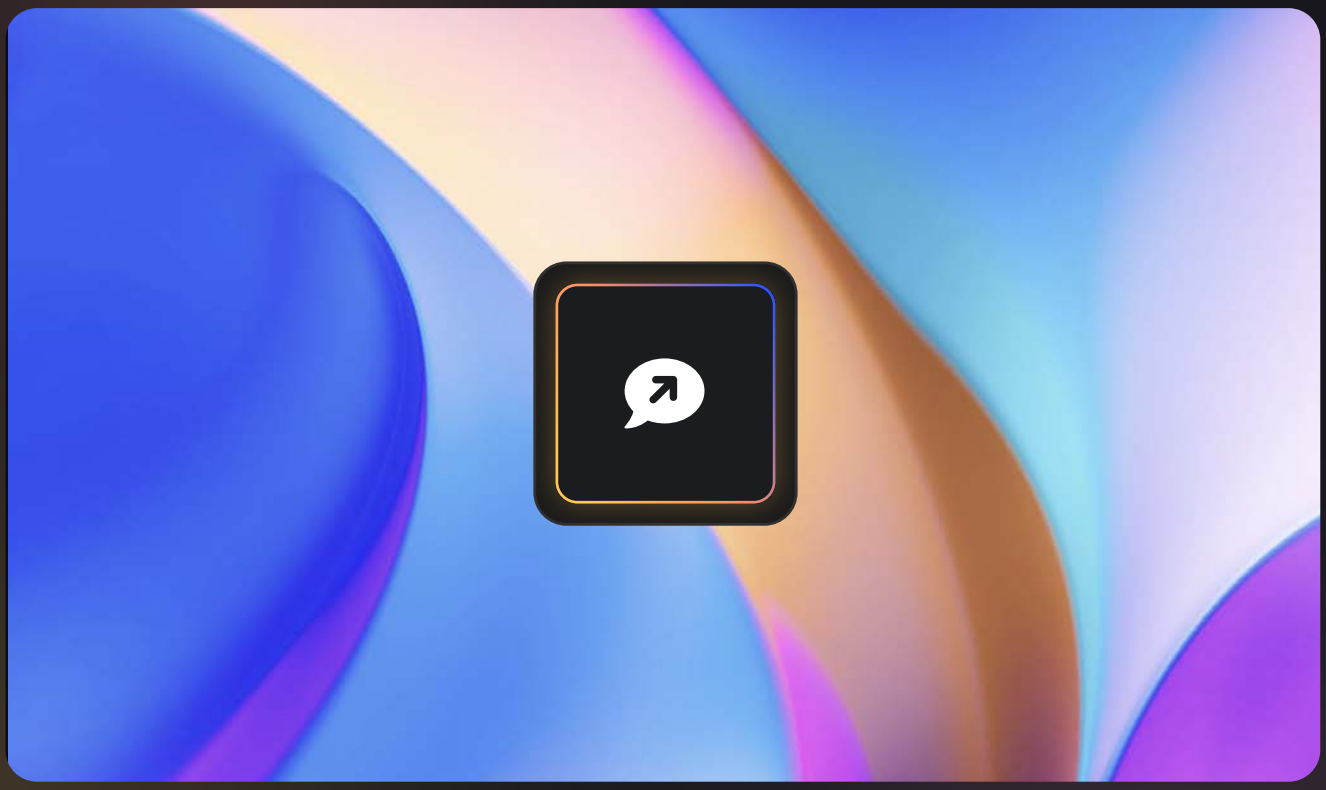
Un des points faibles dans de nombreuses attaques, comme celles basées sur le credential stuffing, est l'utilisation de mots de passe faibles ou réutilisés. Les solutions Mailinblack comprennent également un gestionnaire de mots de passe sécurisés, garantissant que les informations sensibles sont protégées et réduisant les risques liés à des identifiants compromis.

# Formation continue et sensibilisation

La sensibilisation des employés est une composante essentielle de la cybersécurité. Les entreprises peuvent former leurs équipes à reconnaître les signes d'une tentative d'hameçonnage ou d'attaque. C'est grâce à la formation continue et à la sensibilisation à la cybersécurité que les organisations se prémunissent des cyberattaques.


En intégrant U-Cyber 360° dans leur stratégie de cybersécurité, les entreprises peuvent bénéficier d'une solution complète et évolutive, permettant de protéger leurs infrastructures critiques, de minimiser les risques d'attaque et de garantir une réponse rapide et efficace face aux cybermenaces.

# Contactez-nous



contact@mailinblack.com
+33 (0)4 88 60 07 80
www.mailinblack.com
4 place Sadi Carnot, 13002 Marseille

MAILINBLACK