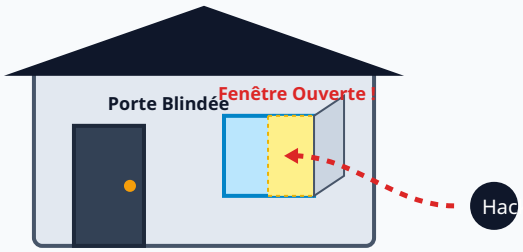
CYBERSÉCURITÉ & ENTREPRISE

Cybersécurité : Les 6 erreurs majeures qui exposent les entreprises aux cyberattaques

Auteur : Alunni Deliora (Ingénieure en cybersécurité) **Temps de lecture :** 7 min **Catégorie :** Bonnes Pratiques & Guide

Lorsqu’on évoque les cyberattaques, l'imagerie populaire convoque souvent des hackers surpuissants exploitant des technologies futuristes et indétectables. La réalité du terrain est pourtant tout autre. La très grande majorité des compromissions ne découle pas d'une prouesse technologique d'une complexité extrême, mais simplement de l'exploitation d'une faiblesse évidente ou négligée.



Analogie : *L'attaquant n'essaiera jamais de défoncer la porte blindée s'il existe une fenêtre ouverte au rez-de-chaussée.*

> *« Imaginez un cambrioleur face à une maison équipée d'une porte blindée de dernier cri. S'il s'aperçoit qu'une fenêtre est restée grande ouverte au rez-de-chaussée, il ne cherchera pas à défoncer la porte : il empruntera le chemin le plus simple, le moins coûteux et le plus efficace. »*

Plutôt que d'aligner du code complexe pendant des heures, revenons aux fondamentaux à travers une analyse concrète des six erreurs critiques qui ouvrent aujourd'hui la voie aux cybercriminels.

1. La négligence dans la gestion des vulnérabilités

Le problème

Une vulnérabilité est une faiblesse ou une faille présente dans un logiciel, un système d'exploitation, une application ou un équipement réseau. Lorsqu'un éditeur découvre une telle faille, il publie un correctif (un « patch »). Dès cet instant, une course contre la montre s'engage : les défenseurs doivent appliquer le correctif tandis que les cybercriminels cherchent activement les systèmes non mis à jour pour les exploiter.

Dans la pratique, appliquer un patch n'est pas toujours aussi simple qu'un clic. Une mise à jour peut créer des incompatibilités, casser des applications métiers critiques ou nécessiter une phase de tests préalable. L'erreur ne réside donc pas dans le fait de ne pas tout mettre à jour instantanément, mais dans l'absence de priorisation intelligente.

Comment opère l'attaquant ?

Les cybercriminels scannent en permanence Internet à la recherche de VPN exposés, de pare-feux non mis à jour, d'interfaces d'administration accessibles et de logiciels vulnérables. La faille technique n'est souvent que la porte d'entrée : une fois à l'intérieur, l'attaquant pivote, cherche des identifiants et s'infiltre plus profondément dans le réseau.

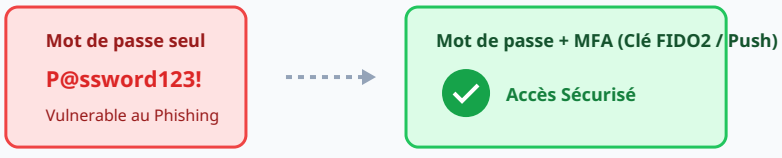
CAS RÉEL : EQUIFAX (2017)

En septembre 2017, l'agence de crédit américaine Equifax subit une fuite massive touchant environ 147 millions de personnes. L'origine de cette attaque historique ? Une vulnérabilité connue et documentée qui n'avait pas été corrigée sur un système exposé, permettant aux attaquants d'accéder progressivement à l'ensemble du réseau.

Les Solutions Recommandées

- **Connaître son patrimoine informatique :** Dresser un inventaire précis des serveurs, postes, équipements réseau, VPN et services cloud. On ne peut pas protéger ce qu'on ne connaît pas.
- **Identifier l'exposition externe :** Cartographier précisément ce qui est accessible depuis Internet.
- **Prioriser :** Traiter en priorité absolue les vulnérabilités critiques et exploitables sur les équipements exposés (ex. VPN).
- **Mettre en place un vrai Patch Management :** Définir clairement les rôles (qui évalue le risque, qui teste, qui valide et dans quel délai).
- **Contrôler après correction :** Vérifier systématiquement que le patch est effectif.

2. La dépendance au simple mot de passe



Évolution : *La complexité ne suffit plus, l'Authentification Multifacteur (MFA) est indispensable.*

Le problème

Pendant des années, le conseil de sécurité majeur consistait à exiger des mots de passe toujours plus complexes (majuscules, minuscules, chiffres, caractères spéciaux, 12, 15 ou 20 caractères). Aujourd'hui, la vraie question n'est plus seulement la complexité du mot de passe, mais : que se passe-t-il si ce mot de passe est volé ? Même un mot de passe très complexe peut être compromis.

Comment opère l'attaquant ?

- **Le Phishing :** Création d'une fausse page d'authentification (ex. Microsoft 365) pour récupérer vos identifiants.
- **Le Credential Stuffing :** Exploitation de fuites de données externes pour tester les combinaisons email/mot de passe réutilisées sur d'autres services.
- **Le Password Spraying :** Test de mots de passe très courants (ex. « Bienvenue2026! ») sur un grand nombre de comptes différents pour éviter le verrouillage.

CAS RÉEL : COLONIAL PIPELINE (2021)

L'attaque majeure ayant paralysé cet opérateur d'oléoducs américain a débuté par la compromission d'un simple mot de passe associé à un ancien compte VPN qui ne bénéficiait pas d'une authentification multifacteur.

Les Solutions Recommandées

- **Déployer l'authentification multifacteur (MFA) :** La MFA ajoute une seconde barrière indispensable. Même si le mot de passe est dérobé, l'attaquant ne peut pas se connecter sans le second facteur (clé de sécurité, application d'authentification, passkey).
- **Évoluer vers des mécanismes renforcés :** Privilégier les solutions résistantes au phishing (passkeys, clés FIDO2).

3. Le piège de l'ingénierie sociale et le nouvel apport de l'IA

Le problème

L'ingénierie sociale vise à manipuler un humain pour l'amener à accomplir une action dangereuse (donner un mot de passe, valider une connexion, effectuer un virement). Historiquement, on apprenait aux collaborateurs à repérer le phishing grâce aux fautes d'orthographe ou de syntaxe. Ce critère est désormais obsolète.

L'intelligence artificielle générative ne crée pas de nouvelles formes d'attaques, mais elle permet d'industrialiser et de crédibiliser à l'extrême les messages piégés : ton professionnel irréprochable, langue parfaite et personnalisation avancée.

Comment opère l'attaquant ?

L'attaque repose sur des ressorts psychologiques : **l'autorité, l'urgence et la confidentialité**. Un exemple classique est la « fraude au président » ou le changement de RIB : un e-mail parfait sollicitant un virement confidentiel et urgent sous pression de temps.

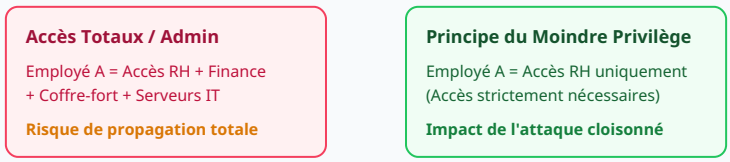
CAS RÉCENTS : FUITES ET ATTAQUES CIBLANT LES SERVICES PUBLICS (2026)

Les fuites de données récentes (comme celles ayant touché des services fiscaux ou l'Éducation nationale) montrent que les données volées (noms, adresses, éléments administratifs) deviennent la matière première des campagnes de phishing de demain. Plus un attaquant détient des détails réels sur votre situation, plus son message frauduleux sera convaincant.

Les Solutions Recommandées

- **Règles de double validation :** Instaurer une procédure hors canal numérique (ex. appel téléphonique de confirmation via un numéro officiel) pour toute modification de coordonnées bancaires ou opération financière.
- **Sensibilisation continue :** Entraîner les équipes à repérer les mécanismes de pression et de manipulation, au-delà de la simple forme du message.
- **Culture de la vérification :** Promouvoir le réflexe « Au moindre doute, je vérifie par un autre canal ».

4. L'octroi de droits d'accès excessifs



Principe du Moindre Privilège : *Ne donnez pas un passe-partout quand une simple clé de chambre suffit.*

Le problème

Imaginez réserver la chambre 26 d'un hôtel et recevoir un badge qui ouvre non seulement la chambre 26, mais aussi la caisse de la réception, la direction et le coffre-fort. En informatique, accorder des droits trop étendus produit exactement le même danger.

Un salarié qui change de poste mais conserve ses anciens accès, un stagiaire doté de privilèges administrateur, ou un compte d'ancien employé non désactivé constituent autant de bombes à retardement.

Les Solutions Recommandées

- **Appliquer le principe du moindre privilège :** Ne donner à chaque utilisateur que les accès strictement nécessaires.
- **Gérer le cycle de vie des comptes :** Arrivée (accès utiles), Mobilité (retrait des anciens droits), Départ (désactivation immédiate).
- **Séparer les comptes :** Cloisonner scrupuleusement les comptes d'administration et les comptes d'usage quotidien.
- **Journalisation :** Enregistrer et surveiller les connexions aux ressources sensibles.

5. La négligence de la sécurité des prestataires et de la chaîne d'approvisionnement (Supply Chain)

Le problème

Une entreprise moderne ne fonctionne pas en vase clos : elle collabore avec des prestataires IT, des éditeurs, des cabinets comptables, des infogéreurs et des sous-traitants. Votre surface d'attaque ne s'arrête donc pas aux limites de votre propre infrastructure. Si un partenaire disposant d'un accès distant à votre réseau est compromis, c'est votre propre entreprise qui devient vulnérable.

CAS RÉEL : SOLARWINDS (2020)

Des attaquants ont compromis le logiciel de gestion de réseau d'un fournisseur légitime pour s'infiltrer chez des milliers d'organisations clientes. En détournant la relation de confiance accordée au prestataire, les pirates ont franchi sans effort les défenses périmétriques.

Les Solutions Recommandées

- **Recenser les accès tiers :** Tenir à jour la liste exacte des prestataires et partenaires ayant un accès distant.
- **Évaluer la stricte nécessité :** Supprimer sans attendre les accès temporaires ou obsolètes.
- **Exiger des standards de sécurité stricts :** Imposer la MFA, des comptes nominatifs et une traçabilité rigoureuse.

6. L'absence ou l'impréparation de la gestion de crise

Le problème

Considérer que l'on est 100 % invulnérable est l'une des erreurs les plus dangereuses. Une organisation mature ne cherche pas seulement à prévenir les attaques : elle se prépare à l'éventualité où une attaque réussirait.

Lorsqu'un ransomware se déclenche un lundi matin, bloquant les fichiers et la messagerie, ce n'est pas le moment d'improviser. Si votre plan de continuité d'activité est stocké sur les serveurs qui viennent d'être chiffrés, il ne vous sera d'aucune utilité.

Les Solutions Recommandées

- **Élaborer un plan de gestion de crise clair :** Définir les rôles, la gouvernance et la communication d'urgence.
- **Garantir des sauvegardes hors ligne :** Conserver des copies isolées (offline) des procédures de crise.
- **Organiser des exercices de crise :** Tester régulièrement vos scénarios de restauration en conditions réelles.

Conclusion : Adopter la défense en profondeur

Pour vous protéger efficacement, l'objectif n'est pas de bâtir une muraille unique et inviolable, mais de déployer une **défense en profondeur** reposant sur l'accumulation de barrières complémentaires :

- Si une vulnérabilité existe, elle doit être rapidement détectée et corrigée.
- Si un mot de passe est volé, la MFA doit bloquer l'accès.
- Si un compte est compromis, le principe du moindre privilège doit limiter les dégâts.
- Si un prestataire est attaqué, ses accès doivent être strictement cloisonnés.
- Si malgré tout une attaque aboutit, une gestion de crise éprouvée et des sauvegardes doivent permettre un rétablissement rapide.

Question pour conclure

Parmi ces six erreurs, laquelle constitue aujourd'hui le risque le plus critique pour votre entreprise, et quelle action concrète pouvez-vous lancer dès demain pour y remédier ?