SÉCURISÉ

Le guide de survie en cybersécurité pour protéger votre entreprise

UNE PUBLICATION AWSMTECH

TABLE DES MATIÈRES

Pourquoi ce guide sur la cybersécurité ?

Sans grande surprise, ce que vous tenez entre les mains — ou lisez sur votre écran — est un guide consacré à la cybersécurité.

Mais pourquoi publier un guide de plus sur un sujet déjà largement traité ?

Parce que beaucoup de dirigeants voient encore la cybersécurité comme un sujet anxiogène qu'ils préféreraient éviter. Pour beaucoup, elle provoque cette même sensation de ventre noué et de gorge serrée que l'on ressent juste avant d'aller chez le dentiste.

Ce sentiment vient souvent de l'inconnu et de nombreuses années de discours alarmistes. Résultat : la cybersécurité reste un sujet périphérique, souvent repoussé derrière des thèmes jugés plus urgents, comme la vente, le marketing ou les opérations.

Après tout, personne n'a envie d'imaginer les scénarios catastrophes auxquels son entreprise — voire sa vie — pourrait être confrontée, surtout lorsqu'il pourrait plutôt se concentrer sur la croissance de son activité.

Le problème, c'est que la peur peut entraîner du « technostress » et de l'apathie. Lorsqu'un problème semble trop vaste ou trop complexe, les dirigeants ont tendance à se sentir impuissants et à décrocher complètement — ce qui, ironiquement, les rend encore plus vulnérables face aux menaces qu'ils redoutent.

Avec cela en tête, je vous promets que ce guide n'a pas pour but de créer une urgence artificielle ni d'utiliser la peur comme levier pour vous pousser à investir dans la cybersécurité.

Son objectif est de démystifier la cybersécurité, de la rendre plus digeste et — au risque d'aller un peu loin — peut-être même intéressante.

Ce guide vise à vous donner la confiance nécessaire pour agir, sans devoir devenir expert. Vous verrez comment fonctionne la cybersécurité et pourquoi elle devient beaucoup plus simple lorsqu'elle s'appuie sur un cadre clair.

En résumé, vous allez découvrir comment renforcer la sécurité de votre entreprise et mieux la protéger contre les cybercriminels opportunistes.

Je ne peux évidemment pas vous promettre que le simple fait de lire ce guide et d'en appliquer les conseils rendra votre entreprise totalement inviolable — ce ne serait pas réaliste. En revanche, cela renforcera considérablement vos défenses.

La vérité, c'est qu'aucune entreprise ni organisation n'est sécurisée à 100 %. Si un prestataire informatique vous affirme le contraire, il n'est probablement pas totalement transparent avec vous.

Même de grands gouvernements, avec toutes leurs ressources sophistiquées, peuvent être touchés par des attaques avancées.

Cela dit, vous pouvez protéger votre entreprise contre la majorité des menaces existantes. Vous serez peut-être même surpris d'apprendre qu'une très grande partie des incidents — 80 à 90 % — provient de choses incroyablement simples et souvent négligées.

La bonne nouvelle, c'est que cela signifie aussi qu'il est relativement simple de mettre en place des mesures de protection efficaces.

Au fil des pages, vous verrez qu'une grande partie de la cybersécurité consiste simplement à adopter de nouvelles habitudes régulières. Des actions simples, concrètes, que vous et votre équipe pouvez intégrer à votre quotidien.

Avancez dans ce guide étape par étape.

Ne vous sentez pas obligé de tout mettre en œuvre d'un seul coup. Choisissez plutôt une ou deux actions pratiques dans chaque chapitre que vous pouvez commencer à appliquer immédiatement. L'objectif principal est de progresser par étapes, plutôt que de viser une perfection impossible du jour au lendemain.

Nous commencerons par poser les bases, puis nous passerons en revue les habitudes les plus importantes pour protéger à la fois vos collaborateurs et vos données les plus précieuses.

Alors, prenez un café — ou votre boisson préférée — et commençons ensemble à construire un avenir plus sûr pour votre entreprise.

Bien à vous,

Andrea C. Nuti
Co-fondateur

PARTIE I

Le quoi & le pourquoi

Ce qu’est la cybersécurité

Je souhaite commencer ce chapitre en clarifiant ce que la cybersécurité n’est pas. Les experts techniques ont souvent tendance à compliquer des sujets simples, et c’est précisément ce que je veux éviter dans ce guide.

Pour un dirigeant d’entreprise, la cybersécurité n’est pas forcément un sujet écrasant de complexité. Il est vrai qu’elle peut devenir très complexe pour les grandes multinationales, les administrations publiques ou les laboratoires scientifiques. Mais si votre entreprise ne traite pas de données hautement sensibles et n’opère pas dans un secteur d’infrastructure critique, la réalité est différente. Pour la plupart des petites et moyennes entreprises, les fondamentaux sont simples et maîtrisables.

La cybersécurité n’est pas un produit que l’on achète. C’est un ensemble de bonnes habitudes pour gérer le risque numérique. Son but est simple : réduire la probabilité et l’impact d’événements qui pourraient perturber vos systèmes, exposer vos données ou nuire à votre activité.

Et la cybersécurité ne fait pas de distinction. Beaucoup de dirigeants pensent que leur entreprise est trop petite pour être ciblée. C’est une hypothèse dangereusement dépassée. La plupart des hackers ne sont pas des génies du crime cherchant à faire tomber un gouvernement. Ils exploitent un modèle basé sur le volume, avec des logiciels automatisés qui scannent l’ensemble d’Internet à la recherche de failles faciles. Votre taille ne vous rend pas invisible ; elle peut même faire de vous une cible plus facile, car les attaquants supposent que vos défenses sont plus faibles. C’est pourquoi 43 % de toutes les cyberattaques visent les petites entreprises[1], et qu’un chiffre alarmant de 60 % d’entre elles ferment dans les six mois suivant une attaque majeure[2].

43%

de toutes les cyberattaques ciblent les petites entreprises

Mais voici le point le plus important : beaucoup de ces attaques ne sont pas des offensives sophistiquées et ultra-technologiques. Elles exploitent des choses simples, souvent négligées. Les données les plus récentes montrent qu’entre 60 % et 95 % des violations impliquent un facteur humain non malveillant[3], comme un collaborateur qui clique accidentellement sur un mauvais lien ou qui se laisse convaincre par un e-mail bien imité. Cela signifie que des mesures de protection simples et efficaces sont totalement à votre portée. Vous avez les moyens de protéger votre entreprise, sans budget à sept chiffres.

Alors, comment se protéger contre ces menaces courantes ? Il suffit d’avoir une manière simple d’y réfléchir. En réalité, toute la cybersécurité repose sur trois piliers essentiels :

Le premier est **l’identité**. Il s’agit de savoir qui possède les clés de votre entreprise : vos collaborateurs, leurs comptes et les appareils qu’ils utilisent. Si vos habitudes sont approximatives — par exemple des mots de

passe partagés ou des accès d'anciens employés toujours actifs — toute votre entreprise devient fragile. Une bonne gestion des identités est votre première ligne de défense.

Le deuxième pilier est **la donnée**. C'est ce que vous cherchez à protéger : vos finances, vos listes clients, votre savoir-faire. Savoir où ces données sont stockées, contrôler qui y a accès et conserver des copies fiables et testées constitue votre filet de sécurité ultime.

Enfin, il y a **les opérations**. C'est la discipline qui consiste à maintenir les systèmes à jour, surveiller les activités inhabituelles et disposer d'un plan lorsque quelque chose tourne mal. C'est là que vivent vos habitudes : par exemple le petit appel téléphonique de deux minutes pour vérifier un changement de coordonnées bancaires avant un paiement, ou la sauvegarde régulière de vos systèmes. Des opérations efficaces garantissent que vos défenses restent actives et prêtes.

Ces trois piliers forment la base d'une cybersécurité efficace. La méthode proposée dans ce guide repose sur deux idées simples : adopter quelques habitudes clés et suivre un plan clair. La plupart des progrès viennent de petites actions répétées régulièrement. Un cadre simple vous aide à garder le cap et à éviter de perdre du temps sur ce qui compte moins.

Cela m'amène au point le plus important : la cybersécurité n'est pas seulement « une affaire d'IT ». C'est une responsabilité de direction. Votre équipe informatique ou votre prestataire IT peut réaliser le travail opérationnel, mais vous devez fixer les priorités, poser les bonnes questions et demander des preuves.

Le retour sur investissement de la cybersécurité

Alors, quel est le retour sur investissement de la cybersécurité ?

La réponse ne se trouvera pas forcément sur votre relevé bancaire — du moins pas si tout se passe comme prévu.

Investir dans la cybersécurité ressemble à investir dans de bonnes serrures pour vos portes ou dans un système anti-incendie pour votre entrepôt.

Vous dépensez un peu d'argent aujourd'hui pour réduire fortement le risque d'une perte beaucoup plus importante — et beaucoup plus douloureuse — demain. En termes business, vous réduisez simplement votre perte attendue.

La formule est simple : **Perte attendue = impact financier de l'incident × probabilité qu'il se produise.**

Tout l'objectif de vos dépenses en cybersécurité consiste à faire baisser fortement ces deux chiffres.

Rendons maintenant cet « impact financier » plus concret, car il ne se limite pas à une demande de rançon.

Commençons par le coût de l'interruption d'activité. Combien coûterait à votre entreprise un arrêt complet de trois jours ?

Par exemple, si votre entreprise réalise habituellement CHF 10'000.00 de chiffre d'affaires par jour, cela représente déjà CHF 30'000.00 de perte.

Ajoutez à cela trois jours de salaires pour une équipe qui ne peut pas travailler, puis toutes les heures supplémentaires nécessaires pour rattraper le retard une fois les systèmes rétablis.

Vient ensuite le risque de vol direct. Cela se produit souvent via de fausses factures ou des comptes e-mail compromis. La perte moyenne liée à ce type d'incident est d'environ **CHF 137'000.00**[4]. Que représenterait, pour votre entreprise ce trimestre, un trou imprévu de CHF 137'000.00 dans votre trésorerie ?

Enfin, il y a les coûts de remise en état. C'est la facture qui arrive une fois l'attaque terminée : experts cyber en urgence, analyses forensiques, restauration des systèmes, conseils juridiques et conformité réglementaire.

Pour les petites et moyennes organisations, les frais de récupération dépassent souvent CHF 10'000.00 et peuvent atteindre CHF 500'000.00. Pour les grandes entreprises, le coût moyen d'un incident atteint USD 4,4 millions au niveau mondial et plus de USD 10 millions aux États-Unis, selon le rapport IBM Cost of a Data Breach 2025[5].

Près d'un tiers des cas impliquent désormais des amendes réglementaires, dont la moitié dépasse CHF 100'000.00.

Lorsque l'on additionne tout, l'impact financier total d'un seul incident peut facilement atteindre plusieurs centaines de milliers de francs — ce qui explique pourquoi tant de petites entreprises ne survivent pas à une attaque.

Alors, comment faire baisser ces chiffres ? En commençant par les investissements qui offrent le retour le plus clair et le plus important.

Pour réduire la probabilité de ces attaques, les données montrent année après année que les attaquants accèdent généralement aux systèmes par quelques portes d'entrée bien connues : mots de passe volés et logiciels obsolètes. Cela vous indique exactement où concentrer vos efforts.

Pour **réduire la probabilité de vol**, commencez par des contrôles d'identité solides.

Le plus important est l'authentification multifacteur (MFA), ce petit code que vous recevez sur votre téléphone lorsque vous vous connectez. Elle bloque la majorité des attaques reposant sur des mots de passe volés. Le coût d'activation de la MFA est minime comparé au transfert frauduleux à six chiffres qui n'aura jamais lieu parce qu'un attaquant n'aura pas pu franchir l'écran de connexion.

Pour **réduire l'impact financier d'un rançongiciel**, vous avez besoin de sauvegardes testées et hors ligne.

Cet investissement peut transformer une crise de plusieurs semaines en une récupération maîtrisable sur un week-end. Lorsque vos fichiers sont verrouillés et qu'un criminel exige une rançon, une copie propre et protégée de vos données change tout.

Alors que **75 % des petites entreprises affirment qu'elles ne pourraient pas continuer à fonctionner en cas d'attaque par rançongiciel**, une sauvegarde testée est votre porte de sortie face à cette statistique.

75%

des petites entreprises ne survivraient pas à une attaque par rançongiciel

Pour **réduire vos coûts de remise en état**, vous avez besoin d'une protection moderne des terminaux et d'une routine pour maintenir vos logiciels à jour.

Les anciens antivirus ne suffisent plus. Les outils modernes recherchent des comportements suspects, et pas seulement des virus déjà connus. Ils peuvent stopper une attaque net, en la contenant à un seul ordinateur au lieu de la laisser se propager à tout votre réseau.

Mais une bonne cybersécurité ne sert pas uniquement à empêcher les mauvaises choses d'arriver ; elle peut aussi devenir un levier de croissance.

La première manière dont elle y contribue est en rendant votre cyber assurance réellement valable. Une cyber assurance n'est pas un chèque en blanc.

Les assureurs exigent désormais que vous disposiez de ces contrôles de base — comme la MFA et les sauvegardes — comme condition de votre police. Si vous ne les avez pas, ils disposent de motifs clairs pour refuser votre demande d'indemnisation, vous laissant seul face à l'impact financier complet de l'incident.

L'autre manière dont elle vous aide à grandir est en vous permettant de remporter des mandats plus importants.

Lorsque vous démontrez une cybersécurité robuste, vous prouvez à vos prospects que vous êtes un partenaire professionnel et fiable, à qui ils peuvent confier leurs données sensibles et leurs opérations en toute confiance.

Cette confiance peut faire la différence dans des appels d'offres concurrentiels et vous permettre de décrocher des contrats rentables qui auraient autrement pu être attribués à des concurrents moins bien sécurisés.

Les menaces les plus courantes

Si vous dirigez une petite ou moyenne entreprise, les cybermenaces auxquelles vous êtes exposé ne ressemblent en rien à ce que l'on voit dans les films.

Les cybercriminels fonctionnent comme une entreprise. Comme vous, ils cherchent des moyens efficaces de gagner de l'argent. Cela signifie qu'ils s'appuient sur un mode opératoire bien rodé : un petit nombre de stratégies fiables, rentables et répétables.

Dans ce chapitre, nous allons examiner ces méthodes, catégorie par catégorie. Nous verrons comment les attaquants ciblent vos collaborateurs, votre technologie et vos opérations quotidiennes. Les comprendre vous aidera à mieux vous protéger.

Catégorie 1 : Menaces visant vos collaborateurs

La plupart des incidents de sécurité ne commencent pas par un hacker qui contourne un pare-feu. Ils commencent par une personne.

Année après année, les données montrent que le « facteur humain » intervient dans la majorité des violations. Le rapport Verizon Data Breach Investigations Report 2025 l'a constaté dans **60 % des incidents**.[6]

Les attaquants savent que votre équipe est votre plus grand atout, et ils exploitent précisément cette force pour trouver une ouverture.

Menace n° 1 : phishing & ingénierie sociale

Au fond, le phishing est une arnaque. Il s'agit d'une attaque trompeuse conçue pour pousser quelqu'un à faire quelque chose qu'il ne devrait pas faire, comme cliquer sur un lien malveillant, ouvrir une pièce jointe dangereuse ou révéler son mot de passe.

La forme la plus courante est la campagne de phishing de masse, où un attaquant envoie des millions d'e-mails génériques en espérant qu'un faible pourcentage de destinataires se fasse piéger. Cela peut prendre la forme de faux avis de livraison FedEx ou d'alertes urgentes du type « Votre compte Microsoft va être suspendu ».

La version la plus dangereuse est toutefois le « spear phishing ».

Dans ce cas, l'attaquant fait ses recherches. Il se renseigne sur votre entreprise, identifie les personnes clés dans des services comme la comptabilité, puis rédige un e-mail personnalisé qui semble venir de vous ou d'un fournisseur de confiance.

Cela mène souvent à la compromission d'e-mail professionnel, ou Business Email Compromise (BEC). C'est l'une des attaques les plus coûteuses pour une petite entreprise. Les attaquants peuvent s'insérer dans une conversation e-mail existante, attendre le bon moment, puis envoyer un message du type : « Bonjour, nous avons mis à jour nos coordonnées bancaires. Merci d'envoyer le paiement de ce mois-ci sur ce nouveau compte. » Comme le message semble légitime, il est très efficace.

Le BEC est un problème massif : il représente près de **2,8 milliards de dollars de pertes déclarées aux États-Unis pour la seule année 2024**, selon le rapport annuel 2024 de l'Internet Crime Complaint Center (IC3) du FBI.

À ce stade, vous vous dites peut-être : « Mes collaborateurs sont trop intelligents pour tomber dans le panneau. » Et vous avez probablement raison. Le problème, c'est que ces attaques ne reposent pas sur l'intelligence.

Elles exploitent les distractions auxquelles nous sommes tous exposés pendant une journée de travail chargée. Les données montrent que lorsqu'une personne se fait piéger par un e-mail de phishing, cela se produit très vite : le temps médian entre la réception de l'e-mail et le clic sur le lien est de **moins de 25 secondes**[7].

Alors, comment vous et votre équipe pouvez-vous reconnaître ces attaques ? Elles partagent presque toujours quelques caractéristiques communes :

- **Un sentiment d'urgence soudain.** L'e-mail crée une pression et vous pousse à agir immédiatement, sous peine de conséquences négatives. Des mots comme « Urgent », « Important » ou « Attention » sont fréquents dans les objets d'e-mails frauduleux. C'est une technique psychologique conçue pour provoquer la panique et contourner les vérifications habituelles.
- **Une demande qui sort du cadre habituel.** Le message vous demandera de faire quelque chose en dehors du processus normal de l'entreprise, souvent avec une raison de garder cela discret. Par exemple : « Je

suis en réunion et je ne peux pas parler, peux-tu simplement payer cette facture pour moi et ne le dire à personne ? »

- **De petites imperfections.** L'adresse e-mail de l'expéditeur peut différer d'une lettre, ou l'adresse de destination affichée lorsque vous survolez un lien avec la souris ne correspond pas au texte visible. Ce sont de petits détails faciles à manquer quand on est pressé.

Menace n° 2 : menaces internes

C'est un sujet sensible, car il concerne des personnes que vous avez engagées et à qui vous avez choisi de faire confiance.

Une menace interne survient lorsqu'un employé actuel ou ancien, un prestataire ou un partenaire utilise ses accès autorisés pour nuire à l'entreprise.

C'est plus courant que beaucoup de dirigeants ne l'imaginent : un rapport de 2024 indique que **48 % des entreprises ont subi des attaques internes plus fréquentes** que les années précédentes[9]. Il est important de comprendre que cela n'est pas toujours malveillant.

Parfois, il s'agit d'une **menace interne involontaire**. C'est le cas d'un collaborateur bien intentionné qui commet une erreur.

Par exemple, il peut envoyer une liste clients sensible sur son compte Gmail personnel pour y travailler pendant le week-end. Son intention n'est pas de nuire, mais il a déplacé des données de l'entreprise hors de votre contrôle, créant ainsi un risque de sécurité.

D'autres fois, il s'agit d'un **interne malveillant**. Cela peut être un collaborateur mécontent sur le point de quitter l'entreprise, qui télécharge une copie de votre base clients pour l'emporter dans son prochain poste. Ou un prestataire dont le projet est terminé, mais dont les accès n'ont jamais été révoqués, lui permettant encore de fouiller dans vos systèmes plusieurs semaines plus tard.

Vous devez faire confiance à votre équipe, mais la mise en place de contrôles de sécurité reste essentielle.

Vous mettez en place des contrôles financiers non pas parce que vous supposez que votre comptable est un voleur, mais parce que c'est la bonne manière de protéger l'argent de l'entreprise. La même logique s'applique à vos données. De bons contrôles protègent l'entreprise contre les actes intentionnels et empêchent les bons collaborateurs de commettre des erreurs accidentelles.

Reconnaître une menace interne peut être difficile, car la personne dispose déjà d'un accès légitime.

Les signes sont généralement des changements de comportement :

- **Accès à des volumes inhabituels de données.** Un collaborateur du marketing qui tente soudainement d'accéder à des plans d'ingénierie, ou quelqu'un qui télécharge des milliers de fichiers juste avant de partir en vacances.
- **Travail à des heures inhabituelles.** Un utilisateur qui travaille normalement de 9 h à 17 h se connecte soudainement à 2 h du matin et accède à des dossiers sensibles.
- **Tentatives de contournement des contrôles de sécurité.** Un collaborateur tente à plusieurs reprises d'accéder à des parties du réseau auxquelles il n'est pas autorisé, ou demande les mots de passe de ses collègues.

Catégorie 2 :
Menaces visant votre technologie & votre chaîne d'approvisionnement

Si de nombreuses attaques commencent par viser vos collaborateurs, elles réussissent presque toujours en exploitant une faille dans votre technologie.

Même si un attaquant obtient le mot de passe d'un collaborateur, il lui faut souvent une « porte » technique pour entrer. C'est là que l'automatisation joue un rôle clé : les criminels scannent Internet en continu à la recherche de failles faciles à exploiter.

Menace n° 3 : utilisation d'identifiants volés

Les noms d'utilisateur et mots de passe de vos collaborateurs sont les clés de votre entreprise. Le problème, c'est que ces clés sont fréquemment copiées et revendues. Lorsqu'une grande entreprise comme LinkedIn ou Adobe subit une fuite de données, les listes de noms d'utilisateur et de mots de passe volés apparaissent souvent en vente sur le dark web.

Les criminels achètent ces énormes listes, puis utilisent des logiciels automatisés pour tester les mêmes combinaisons d'identifiants et de mots de passe sur d'autres sites, comme la page de connexion à la messagerie de votre entreprise.

C'est ce que l'on appelle le « credential stuffing », et cela fonctionne parce que les gens réutilisent leurs mots de passe. Une étude récente a montré que **49 % des employés réutilisent les mêmes identifiants**[9] sur différentes applications liées au travail.

Si votre collaborateur a utilisé le même mot de passe pour son ancien compte Myspace que pour le système de paie de votre entreprise, une fuite datant d'il y a dix ans peut soudain devenir votre problème aujourd'hui.

Cela peut sembler exagéré, mais les identifiants volés sont utilisés dans **86 % des attaques contre les applications web**[10].

Alors, comment reconnaître que cela est en train de se produire ? Voici les signes à surveiller :

- **Alertes de connexion à des heures ou depuis des lieux inhabituels.** Vous pourriez recevoir un e-mail de Microsoft indiquant que quelqu'un a tenté de se connecter à votre compte depuis un autre pays à 3 h du matin.
- **Être bloqué hors de son propre compte.** Si un attaquant tente à plusieurs reprises de se connecter avec un mauvais mot de passe, le système peut verrouiller le compte pour des raisons de sécurité, vous empêchant même vous d'y accéder.
- **Voir une activité que vous ne reconnaissez pas.** Vous pouvez remarquer des e-mails dans votre dossier « envoyés » que vous n'avez pas écrits, ou constater que des fichiers ont été consultés ou téléchargés alors que vous ne travailliez pas.

Menace n° 4 : exploitation de portes numériques restées ouvertes

Ce type d'attaque progresse très vite. Le principe est simple : les hackers recherchent en continu des portes ouvertes sur Internet. Le rapport Verizon Data Breach Investigations Report 2025 indique que ces attaques, utilisées comme première étape d'une violation, ont augmenté de **34 %** par rapport à l'année précédente.

Il existe deux grands types de « portes ouvertes » qu'ils recherchent.

Le premier est celui des **vulnérabilités logicielles**. Imaginez qu'un constructeur automobile découvre une serrure défectueuse sur l'un de ses modèles et lance un rappel. Dès que ce rappel est annoncé, les voleurs savent exactement quoi rechercher.

La même chose se produit avec les logiciels. Lorsqu'une entreprise comme Microsoft ou Google découvre une faille de sécurité dans son produit, elle publie un correctif, aussi appelé mise à jour de sécurité.

Dès que ce correctif est annoncé, les criminels lancent des scans automatisés sur l'ensemble d'Internet, à la recherche des entreprises qui ne l'ont pas encore installé. Avec près de **21'500 nouvelles vulnérabilités logicielles publiées rien que durant le premier semestre 2025**[11], les criminels disposent d'un flux constant de nouvelles portes à tester.

Le deuxième type de porte ouverte concerne les **services d'accès à distance mal configurés**. Ce sont les outils que votre équipe utilise pour travailler hors du bureau, comme un VPN ou le protocole Remote Desktop (RDP). Ces outils sont essentiels pour les entreprises modernes, mais s'ils sont configurés avec des mots de passe faibles ou par défaut, ou s'ils ne sont pas protégés par une authentification multifacteur, ils deviennent une porte grande ouverte visible depuis tout Internet.

Les criminels peuvent exploiter une nouvelle vulnérabilité en quelques heures, alors qu'une organisation moyenne met environ **55 jours à corriger seulement la moitié de ses failles critiques**[12]. Cet écart énorme constitue la fenêtre d'opportunité que les attaquants exploitent.

Et la seule preuve qu'une personne est entrée par un logiciel non corrigé ou une connexion à distance mal sécurisée est souvent ce qu'elle fait ensuite : installer un rançongiciel et verrouiller tous vos fichiers.

8 Menace n° 5 : compromission de la chaîne d'approvisionnement

Votre entreprise ne fonctionne pas seule. Vous travaillez avec des prestataires externes et utilisez de nombreux outils logiciels. Une attaque de la chaîne d'approvisionnement se produit lorsqu'un criminel compromet l'un de ces partenaires de confiance, puis utilise son accès légitime pour atteindre vos systèmes.

C'est une tactique de plus en plus populaire et efficace. Pourquoi attaquer cent petites entreprises une par une lorsqu'il est possible d'attaquer le logiciel unique qu'elles utilisent toutes et d'y accéder en une seule fois ?

Les données montrent qu'il s'agit d'un problème en forte croissance. Les attaques de la chaîne d'approvisionnement ont doublé en fréquence depuis le début de 2025, avec une moyenne de 26 incidents par mois visant des organisations dans le monde entier.

Aujourd'hui, environ 45 % des organisations ont été ciblées via des vecteurs liés à la chaîne d'approvisionnement. Les violations impliquant un tiers représentent désormais environ 30 à 35,5 % de tous les incidents, soit une hausse d'environ 6,5 à 11 % d'une année sur l'autre.[13]

Les accès de tiers sont également responsables de plus de 41 % des attaques par rançongiciel, ce qui fait de la sécurité des fournisseurs un point d'attention essentiel aujourd'hui.[14]

Et si vous pensez que la sécurité de vos fournisseurs n'est pas votre problème, ce n'est plus vrai dans une entreprise moderne et connectée.

Votre sécurité n'est aussi solide que le maillon le plus faible de votre chaîne d'approvisionnement. Si votre prestataire de paie est compromis, les données de vos collaborateurs sont en danger. Si votre prestataire informatique est compromis, les attaquants pourraient obtenir les clés de tout votre royaume numérique. Vous devez considérer vos fournisseurs clés comme une extension de votre propre entreprise et leur imposer un niveau de sécurité raisonnable.

Reconnaître une attaque de la chaîne d'approvisionnement est extrêmement difficile, car l'attaque provient souvent d'une source que vous considérez déjà comme fiable :

- **Une notification de violation de la part de votre fournisseur.** Souvent, vous apprendrez l'existence du problème lorsqu'un fournisseur vous enverra un e-mail indiquant qu'il a subi un incident de sécurité et que vous pourriez être concerné.
- **Une activité suspecte depuis un compte légitime.** Vous pourriez voir l'un des comptes utilisateur de votre fournisseur se connecter à des heures inhabituelles ou tenter d'accéder à des parties de votre système qu'il n'utilise normalement pas. Comme le compte est légitime, cela peut être très difficile à repérer.
- **Vos outils de sécurité signalent une application de confiance.** Votre protection des terminaux peut soudainement identifier comme malveillante une mise à jour habituelle provenant d'un logiciel de confiance. Cela peut arriver lorsqu'un attaquant a réussi à injecter son propre code malveillant dans une mise à jour logicielle légitime.

Catégorie 3 : Menaces visant vos opérations

Une fois qu'un attaquant a franchi la barrière de vos collaborateurs et de votre technologie, son étape suivante consiste à perturber vos opérations et à transformer son accès en source de revenus. Ce sont les menaces qui ciblent directement votre capacité à générer du chiffre d'affaires, servir vos clients et maintenir votre entreprise ouverte.

Menace n° 6 : logiciel malveillant & rançongiciel

Le terme malware désigne tout logiciel malveillant qu'un attaquant installe après avoir obtenu un accès. Il peut s'agir d'un logiciel espion qui vole des informations sur vos ordinateurs, ou d'un enregistreur de frappe qui capture ce que vous tapez.

Souvent, ce type de logiciel malveillant fonctionne en arrière-plan pendant des semaines, voire des mois, en collectant des informations et en donnant à l'attaquant une vision claire de votre entreprise.

Mais le type de malware qui fait le plus parler de lui est le rançongiciel, et pour de bonnes raisons.

Le rançongiciel est la charge finale : un logiciel malveillant conçu avec un modèle économique.

Une fois que l'attaquant a exploré votre réseau, il lance le rançongiciel, qui se propage rapidement et chiffre tous vos fichiers importants. Tout est verrouillé, et le seul moyen de récupérer les données consiste à payer l'attaquant pour obtenir une clé de déchiffrement.

Pour augmenter la pression, les attaquants volent souvent d'abord une copie de vos données. Ils menacent ensuite de les publier si vous ne payez pas. C'est ce que l'on appelle la « double extorsion ». Dans certains cas, ils ajoutent encore une pression supplémentaire, par exemple en ciblant des tiers ou en lançant une attaque par déni de service.

Alors, comment reconnaître ces menaces ?

- **Le logiciel malveillant** est souvent difficile à remarquer. Les signes peuvent être subtils : ordinateurs anormalement lents, fenêtres pop-up étranges, plantages fréquents ou logiciels que vous ne vous souvenez pas avoir installés. Un logiciel malveillant peut aussi provoquer une activité réseau inhabituelle ou désactiver vos outils de sécurité, ce qui rend sa détection difficile sans une surveillance adéquate.
- **Le rançongiciel**, lui, est tout l'inverse. Les signes sont impossibles à manquer. Vous voyez une demande de rançon à l'écran, et plus aucun de vos fichiers ne s'ouvre. Il est conçu pour provoquer un arrêt de travail immédiat et total.

Menace n° 7 : attaques par déni de service (DoS/DDoS)

Toutes les attaques ne visent pas à voler des données ou de l'argent. Certaines cherchent simplement à provoquer une interruption.

Imaginez que votre entreprise dispose d'une seule ligne téléphonique et qu'un plaisantin organise l'appel simultané de cent personnes, encore et encore.

Vos vrais clients ne pourraient plus vous joindre. C'est essentiellement ce qu'une attaque par déni de service (DoS) fait à votre site web ou à vos services en ligne. Elle les inonde d'un tel volume de trafic inutile qu'ils sont saturés et deviennent indisponibles pour les clients légitimes.

Lorsque ce trafic inutile provient simultanément de milliers d'ordinateurs répartis dans le monde entier, on parle d'attaque par déni de service distribué (DDoS).

Le nombre et l'ampleur de ces attaques ont fortement augmenté. Au premier semestre 2025, les incidents DDoS ont progressé de **plus de 40 % sur un an au niveau mondial**, certains rapports faisant même état d'une hausse de 108 % dans certaines régions.[16]

La plus grande attaque enregistrée à la mi-2025 a atteint un pic de 7,3 térabits par seconde, impliquant **des centaines de milliers d'appareils dans le monde entier.**[17]

Alors, comment reconnaître une attaque DoS ou DDoS ?

- Votre site web ou vos systèmes en ligne deviennent soudainement extrêmement lents, ou totalement inaccessibles pour vos clients légitimes.
- Vous pouvez constater une forte augmentation du trafic Internet, souvent bien au-delà des volumes habituels.
- Vous pouvez recevoir un e-mail ou un message de l'attaquant exigeant un paiement pour arrêter le flot de trafic, une tactique d'extorsion courante.

Suivre un cadre de référence — Suisse : standard minimal TIC du NCSC + nLPD

En Suisse, la base la plus pragmatique est le **standard minimal TIC** publié par le **Centre national pour la cybersécurité (NCSC)**. Il propose des mesures concrètes, soutenues par la Confédération et applicables à tous les secteurs. Son objectif est de renforcer la résilience et de réduire les risques cyber les plus courants.

Pour la **protection des données**, les entreprises suisses qui traitent des données personnelles doivent respecter la **nLPD**, en vigueur depuis le **1er septembre 2023**. Selon vos clients et vos marchés, le RGPD peut aussi s'appliquer. Ces règles exigent notamment de limiter les données collectées, de les protéger correctement et de réagir en cas de violation.

Si vous opérez dans des **secteurs réglementés**, par exemple la banque ou l'assurance, votre programme doit aussi tenir compte des circulaires **FINMA**, en particulier la circulaire **2018/3 Outsourcing** pour la gouvernance des tiers, ainsi que la circulaire **2023/1 Risques et résilience opérationnels** pour la gestion et les tests des risques TIC et cyber.

Les exploitants d'infrastructures critiques — énergie, transports publics, eau, etc. — doivent anticiper les obligations de **signalement obligatoire des incidents** introduites dans le cadre des réformes suisses sur la sécurité de l'information, ainsi que les standards minimaux TIC propres à certains secteurs. Certains sont déjà **contraignants**, par exemple pour l'électricité depuis le **1er juillet 2024** et pour le gaz depuis le **1er juillet 2025**. Même si vous n'êtes pas directement concerné, ces standards constituent d'excellentes lignes directrices pour les PME.

CE QUE CHAQUE ÉLÉMENT SIGNIFIE POUR VOTRE ENTREPRISE

L'approche suisse se veut volontairement pratique et évolutive. Elle vous donne des objectifs clairs et des preuves reconnues lorsque des clients, des auditeurs ou des assureurs vous demandent comment vous gérez le risque cyber.

Vous pouvez choisir — ou combiner — plusieurs de ces **voies crédibles** :

- **Standard minimal TIC du NCSC — socle de base.** Mettez en œuvre l'ensemble des contrôles autour des fonctions **Identifier, Protéger, Détecter, Répondre, Récupérer** et utilisez l'outil officiel d'autoévaluation Excel pour mesurer votre maturité, combler les écarts et, si souhaité, faire réaliser un audit externe. C'est rapide, spécifique à la Suisse et peu coûteux.
- **ISO/IEC 27001:2022 — certification SMSI.** Mettez en place un **système de management de la sécurité de l'information** fondé sur les risques et faites-le certifier par un organisme accrédité par le SAS. ISO 27001 est largement reconnue, s'aligne bien avec les attentes de gouvernance de la nLPD et du RGPD, et ouvre des portes auprès de grands acheteurs et de partenaires réglementés. ISO propose même un guide PME pour faciliter l'adoption.
- **Compléments sectoriels — si applicable.** Pour la finance, alignez l'externalisation, l'auditabilité, les inventaires, les exigences transfrontalières et les exigences de sécurité avec **FINMA 2018/3**. Pour la résilience opérationnelle et les tests, appuyez-vous sur **FINMA 2023/1**. Pour les infrastructures critiques, adoptez le **standard minimal TIC** de votre secteur et préparez-vous aux obligations de **notification rapide des incidents**.

En résumé : choisissez un socle de base, comme le standard minimal du NCSC. Ajoutez les obligations de protection des données, notamment la nLPD et, si nécessaire, le RGPD. Puis complétez avec ISO 27001 ou les règles sectorielles lorsque votre activité l'exige. Cette approche par couches donne une feuille de route claire.

Les cinq contrôles pratiques — adaptés à la Suisse

Votre liste de contrôles s'aligne très bien avec les recommandations suisses. Voici la version adaptée, avec des actions concrètes et les liens réglementaires utiles :

1. **Périmètre réseau & pare-feu.** Maintenez une frontière renforcée entre votre réseau interne et Internet, ainsi qu'entre les différents segments internes. Documentez les règles entrantes et sortantes, appliquez le principe du refus par défaut et formalisez la gestion des changements. Pour les entreprises réglementées, assurez-vous que les services de périmètre externalisés respectent les exigences contractuelles, de sécurité et d'audit de **FINMA 2018/3**.
2. **Configuration sécurisée.** Appliquez des configurations de référence sécurisées pour les serveurs, postes de travail, services SaaS et environnements cloud : suppression des services inutiles, changement des paramètres par défaut, chiffrement des données sensibles au repos et en transit, sécurisation des appareils mobiles et suivi des dérives de configuration. Le standard minimal du NCSC détaille ces éléments de **défense en profondeur**, notamment le cycle de vie du matériel et la configuration mobile.
3. **Contrôle des accès — moindre privilège & authentification forte.** Appliquez le principe du moindre privilège, l'accès basé sur les rôles et l'**authentification multifacteur (MFA)** sur tous les services exposés à Internet et les comptes administrateurs. Lorsque c'est possible, privilégiez des méthodes résistantes au phishing. Les bonnes pratiques techniques du NCSC britannique peuvent aussi servir de complément utile aux équipes suisses.
4. **Protection contre les malwares — EDR/XDR & sécurité e-mail.** Utilisez une protection moderne des terminaux, segmentez les réseaux et mettez en place l'authentification des e-mails — **SPF, DKIM, DMARC** — afin de réduire l'usurpation de marque, un problème fréquent dans les campagnes de phishing. De nombreux serveurs de réception pénalisent de plus en plus les domaines sans authentification ; considérez DMARC comme un standard de base.
5. **Gestion des correctifs & des vulnérabilités.** Tenez un inventaire des actifs et dépendances, priorisez les CVE et appliquez rapidement les correctifs, surtout sur les systèmes exposés à Internet. Les outils et checklists du NCSC pour les PME mettent l'accent sur les correctifs, les sauvegardes et la MFA comme premières mesures permettant de réduire fortement le risque.

Conseil : si vous traitez des données personnelles, l'application des correctifs et le durcissement des systèmes soutiennent aussi les « mesures techniques et organisationnelles appropriées » exigées par la **nLPD** et réduisent la probabilité d'une violation — ainsi que le besoin de notification au PFPDT.

METTRE LE CADRE EN PRATIQUE

Comme le **standard minimal du NCSC** est un socle reconnu par les autorités suisses, il vous donne une réponse prête à l'emploi et crédible lorsque des clients vous interrogent sur votre sécurité. Il fournit également une checklist concrète à revoir chaque année. De nombreux secteurs — et assureurs — voient favorablement une certification ISO 27001 ou un alignement démontrable avec les contrôles du NCSC.

Réaliser l'évaluation oblige à mettre en œuvre les fondamentaux, en transformant des objectifs vagues en un **plan d'action concret** lié à vos risques et à vos processus métier. Ces preuves peuvent vous aider à négocier de meilleures conditions avec les cyberassureurs et à répondre aux exigences de due diligence de grands clients suisses ou européens, notamment lorsque le **RGPD et la nLPD** s'appliquent tous deux.

Comparer les cadres de référence

Au-delà du socle suisse du NCSC et du standard mondial ISO 27001, abordés plus en détail dans ce guide, trois autres cadres méritent d'être connus. Selon votre marché et les attentes de vos clients, l'un d'eux peut être plus adapté à votre situation — ou constituer un complément utile au cadre que vous avez déjà choisi.

Cadre	Le plus adapté pour	Fonctionnement	Reconnaissance
NIST CSF 2.0 (US)	Entreprises américaines, en particulier celles qui vendent à des clients gouvernementaux ou à de grandes entreprises	Six fonctions : Gouverner, Identifier, Protéger, Détecter, Répondre, Récupérer	Le standard de facto aux États-Unis — correspond à la plupart des questionnaires de sécurité
CIS Controls v8.1 (Global)	Entreprises disposant de ressources IT limitées et souhaitant une liste d'actions priorisées	3 groupes de mise en œuvre ; IG1 couvre 56 actions essentielles et fondamentales	Pratique, neutre vis-à-vis des fournisseurs, largement utilisé par les MSP
Cyber Essentials (UK)	Entreprises travaillant avec le gouvernement britannique ou de grandes entreprises au Royaume-Uni	5 contrôles techniques, autoévalués ou testés de manière indépendante avec la version Plus	Soutenu par le gouvernement britannique ; souvent exigé contractuellement

Quel que soit votre choix, l'objectif reste le même : choisissez un cadre, appliquez-le de manière cohérente et utilisez-le comme réponse prête à l'emploi lorsqu'un client, un partenaire ou un assureur vous demande comment vous gérez le risque cyber.

Suivre un cadre de référence — Monde : ISO 27001

Lorsque vous construisez un programme de cybersécurité, il est facile de se perdre dans les détails ou d'acheter des outils dont vous n'avez pas besoin. Un cadre de cybersécurité reconnu permet d'éviter cela.

Si vous souhaitez travailler avec de grandes entreprises ou vendre à des clients à l'international, on vous demandera tôt ou tard ce que vous faites en matière d'**ISO 27001**. Considérez-la comme le standard mondial de référence pour prouver que vous prenez la sécurité de l'information au sérieux. C'est une norme internationale qui démontre que vous disposez d'un système complet et professionnel pour gérer la sécurité.

Contrairement à une simple checklist, ISO 27001 consiste à construire un **système de management de la sécurité de l'information (SMSI)**. Dit simplement, c'est le mode d'emploi de votre entreprise pour gérer la sécurité : qui fait quoi, avec quels processus, quels outils et quelles preuves.

Ce que cela signifie pour votre entreprise

La meilleure façon de comprendre le cadre ISO 27001 est de le voir comme un cycle continu en quatre étapes simples : **Planifier, Déployer, Contrôler et Améliorer (PDCA)**. Ce cycle est le moteur de tout votre programme de sécurité : il garantit que vous ne mettez pas les choses en place une fois pour ensuite les oublier, mais que vous vous améliorez en continu.

- **Planifier :** c'est ici que vous déterminez ce que vous devez protéger et quels sont les plus grands risques pour ces informations. Vous créez un inventaire de vos données importantes, identifiez les menaces potentielles — comme un rançongiciel ou une erreur humaine — et établissez un plan simple pour traiter ces risques. C'est la partie stratégique de votre programme de sécurité.
- **Déployer :** c'est ici que vous mettez votre plan en action. Vous appliquez les contrôles et les habitudes de sécurité évoqués dans ce guide, comme activer l'authentification multifacteur, mettre en place vos sauvegardes et former votre équipe. Vous rédigez aussi des politiques simples, en langage clair, qui décrivent vos règles de sécurité.
- **Contrôler :** c'est ici que vous vérifiez votre travail pour vous assurer que le plan fonctionne. Vous réalisez par exemple des audits internes et organisez des réunions régulières de direction pour revoir votre sécurité. Les règles sont-elles suivies ? Les outils de sécurité fonctionnent-ils correctement ?
- **Améliorer :** c'est ici que vous corrigez les problèmes identifiés lors de l'étape « Contrôler » et que vous améliorez les choses. Si vous trouvez une faille dans votre sécurité, vous créez un plan pour la combler. C'est la partie « amélioration continue » du cycle, celle qui maintient votre programme de sécurité efficace dans le temps, à mesure que votre entreprise et les menaces évoluent.

METTRE LE CADRE EN PRATIQUE

Le plus grand avantage d'ISO 27001 est sa reconnaissance mondiale. Lorsqu'un grand prospect vous envoie un long questionnaire de sécurité, pouvoir répondre « Nous sommes certifiés ISO 27001 » suffit souvent à clore la discussion et à satisfaire ses exigences. C'est un signal crédible et compris internationalement : vous êtes un partenaire professionnel et digne de confiance. Cela peut raccourcir votre cycle de vente et vous aider à remporter des mandats que vous auriez autrement perdus.

L'alternative à un cadre, c'est ce que font la plupart des entreprises : elles réagissent.

Une actualité inquiétante sur les rançongiciels sort, et elles achètent un nouvel outil de sauvegarde. Elles entendent parler de phishing, et elles lancent une formation. Cette approche donne l'impression d'agir, mais elle laisse souvent de grandes failles invisibles. Un cadre vous donne une vue d'ensemble et un chemin logique.

Il vous oblige aussi à vous organiser. Le processus de certification exige de documenter vos processus clés et de désigner des responsables pour les tâches importantes. Cela apporte souvent des bénéfices bien au-delà de la sécurité, en vous aidant à gérer une entreprise plus efficace et plus prévisible. Vous construisez proactivement une entreprise plus résiliente. C'est précisément le rôle d'un cadre.

Une courte note avant de poursuivre : la prochaine partie de ce guide vous guidera à travers les actions et contrôles concrets à mettre en œuvre, c'est-à-dire le « comment faire » pour des sujets comme la MFA, les sauvegardes et la sécurisation de vos appareils.

Ma recommandation forte est de ne pas mettre ces actions en place au hasard. Intégrez-les au cadre que nous venons de voir. Ainsi, vous disposez d'un chemin clair et vous travaillez toujours d'abord sur ce qui compte le

plus. Cela facilite aussi fortement la preuve de votre sécurité auprès de grands clients ou de votre assureur, car vous pouvez démontrer que vous suivez un standard reconnu.

PARTIE II

Les contrôles prioritaires

Personnes & identité

Votre entreprise possède des actifs numériques importants : listes clients, prix, plans commerciaux. Sans une bonne organisation, ces informations peuvent sortir de l'entreprise lorsqu'un collaborateur part — ou pire, être volées lors d'une cyberattaque.

Ce chapitre vous montre comment contrôler qui accède à vos systèmes et à vos données, afin que vos informations clés restent protégées.

Toutes les personnes qui travaillent pour vous — collaborateurs, prestataires, voire votre fiduciaire — ont besoin d'un accès spécifique pour faire leur travail. Les logiciels que vous utilisez doivent aussi souvent communiquer avec d'autres applications.

L'objectif est de s'assurer que chaque personne et chaque outil n'accèdent qu'à ce qui est nécessaire, et uniquement aussi longtemps que nécessaire. Par exemple, votre équipe commerciale a besoin du logiciel de vente, mais elle ne devrait pas consulter les dossiers de paie. Lorsqu'un mandat de prestataire se termine, ses accès doivent être supprimés immédiatement.

Vous ne laisseriez pas un ancien collaborateur garder les clés de vos bureaux. C'est exactement la même logique pour vos systèmes numériques.

CE QU'IL FAUT FAIRE

Quatre habitudes de base suffisent pour obtenir un impact maximal avec un effort raisonnable. Si vous les appliquez correctement, vous corrigerez une grande partie des problèmes évoqués précédemment.

1. Utiliser l'authentification multifacteur (MFA).

Vous utilisez probablement déjà la MFA tous les jours avec votre application bancaire. C'est le code supplémentaire que vous recevez sur votre téléphone après avoir saisi votre mot de passe. La MFA est simplement une deuxième vérification pour confirmer que c'est bien vous. Votre mot de passe est la première vérification — « quelque chose que vous connaissez » — et le code sur votre téléphone est la deuxième — « quelque chose que vous possédez ».

Un criminel peut voler votre mot de passe, mais il lui est beaucoup plus difficile d'avoir aussi votre téléphone.

La MFA est importante parce que les mots de passe sont souvent volés. La question n'est pas de savoir si les mots de passe de vos collaborateurs seront exposés, mais quand — et combien.

Sans MFA, un criminel qui récupère le mot de passe réutilisé d'un collaborateur peut facilement accéder à vos systèmes. Avec la MFA, ce mot de passe volé devient inutile. Le criminel peut avoir le mot de passe, mais lorsqu'il tente de se connecter, le système lui demande le code du téléphone de votre collaborateur, ce qui bloque l'attaque dès l'entrée.

C'est la meilleure action individuelle que vous puissiez mettre en place pour protéger votre entreprise. Il n'est pas exagéré de dire que ce seul contrôle bloque la majorité des cyberattaques.

Les chiffres sont clairs :

- Microsoft indique que l'utilisation de la MFA bloque **99,9 % des attaques automatisées par mot de passe**. C'est presque une solution miracle en matière de sécurité.

99,9 %

des attaques automatisées par mot de passe sont bloquées par la MFA

- Le rapport Verizon Data Breach Investigations Report 2025 a constaté que les mots de passe volés étaient utilisés dans **88 % des attaques contre les applications web**. La MFA bloque directement cette méthode d'attaque majeure.

Même avec cela en tête, un rapport récent indique que près de **la moitié des petites et moyennes entreprises s'appuient encore uniquement sur les mots de passe**, sans utiliser l'authentification multifacteur.[18]

C'est le plus grand écart entre une bonne sécurité et ce que les entreprises font réellement.

C'est aussi pourquoi votre compagnie de cyberassurance l'exigera presque certainement. Ce n'est plus une option.

Pour obtenir une cyberassurance — ou, plus important encore, pour qu'une demande d'indemnisation soit acceptée en cas d'incident — vous devrez prouver que vous utilisez la MFA sur vos systèmes importants, en particulier votre messagerie et tous les accès à distance. C'est devenu indispensable pour toute entreprise moderne.

2. Utiliser un gestionnaire de mots de passe professionnel.

Soyons réalistes avec les mots de passe. Une personne moyenne en gère des dizaines, et pour certains postes, on se rapproche plutôt de la centaine. Se souvenir d'autant de mots de passe uniques et complexes est impossible. Les gens prennent donc des raccourcis : ils réutilisent les mêmes mots de passe, font de petites variations, utilisent des informations personnelles comme le prénom de leur enfant ou de leur animal, ou les notent sur des post-it.

Chercher des raccourcis fait partie de la nature humaine ; vous ne pourrez pas l'empêcher. Mais ces habitudes créent un risque de sécurité majeur pour votre entreprise.

Les données montrent clairement que les mots de passe faibles ou volés sont à l'origine de la plupart des violations en entreprise.

Au lieu de simplement dire à votre équipe « utilisez de meilleurs mots de passe », vous devez lui donner un outil qui les gère pour elle : un gestionnaire de mots de passe professionnel.

Il s'agit d'un programme sécurisé dans lequel votre équipe peut créer, enregistrer et partager des mots de passe en toute sécurité. Chaque collaborateur dispose de son propre compte chiffré et ne doit retenir qu'un seul mot de passe maître solide pour l'ouvrir.

Le gestionnaire de mots de passe fait le reste : il crée des mots de passe aléatoires et impossibles à deviner pour chaque site et chaque application utilisés, puis les mémorise tous.

C'est important pour plusieurs raisons.

Premièrement, cela règle complètement le problème de la réutilisation des mots de passe. Lorsque chaque site dispose de son propre mot de passe unique et solide, une fuite de données chez une autre entreprise ne vous impacte pas. Si le mot de passe LinkedIn d'un collaborateur est volé, cela n'a pas d'importance, car le mot de passe de sa messagerie professionnelle est totalement différent.

Deuxièmement, cela évite l'utilisation de mots de passe faibles et faciles à deviner. Aussi surprenant que cela puisse paraître, des mots de passe courants comme « 123456 » ou « password » sont encore largement utilisés. Un gestionnaire de mots de passe rend simple l'utilisation d'un mot de passe complexe comme « Tr0c3[sub4dour&R3fls2za@eX! » pour chaque site, car l'utilisateur n'a pas besoin de le retenir.

Les chiffres montrent l'ampleur du problème :

- Environ **la moitié des employés déclarent réutiliser leurs mots de passe** sur différentes applications professionnelles[19].
- Près de **60 % des adultes utilisent des informations personnelles**, comme des prénoms ou des dates d'anniversaire, dans leurs mots de passe, ce qui les rend extrêmement faciles à deviner pour un attaquant.
- Même en 2025, « 123456 » reste le mot de passe le plus utilisé au monde, apparaissant dans des millions de comptes compromis[20].

Un gestionnaire de mots de passe professionnel fournit aussi un moyen sûr de gérer les comptes partagés. Pensez aux comptes de réseaux sociaux de votre entreprise ou à un accès fournisseur partagé.

Comment partagez-vous ces mots de passe aujourd'hui ? Dans un tableur ? Par e-mail ? Il vaut mieux éviter.

Un gestionnaire de mots de passe vous permet de donner accès à cet identifiant à certains membres de l'équipe sans qu'ils voient jamais le mot de passe lui-même. Lorsqu'un collaborateur quitte l'entreprise, vous pouvez supprimer son accès à tous les comptes partagés en un clic, transformant un processus risqué en processus maîtrisé.

3. Appliquer le principe du moindre privilège.

Un collaborateur ne devrait disposer que du niveau d'accès strictement nécessaire pour faire son travail, rien de plus.

Votre responsable marketing a besoin des comptes de réseaux sociaux et du dossier marketing, mais pas de votre logiciel comptable.

Votre équipe commerciale a besoin du logiciel de gestion de la relation client (CRM), mais elle ne devrait pas accéder aux dossiers RH des collaborateurs.

Cela paraît évident, mais dans beaucoup d'entreprises, les accès sont accordés trop largement « au cas où » quelqu'un en aurait besoin, puis ils sont rarement revus ou supprimés.

Avec le temps, presque tout le monde finit par pouvoir accéder à presque tout. Une étude a montré que, dans une entreprise typique, des milliers de fichiers sensibles sont accessibles à l'ensemble des collaborateurs.

Ce principe est important parce que, si le compte d'un collaborateur est compromis, les dégâts restent limités.

Si un attaquant vole le mot de passe d'un membre de votre équipe commerciale, son premier objectif sera de se déplacer dans votre réseau pour trouver des éléments de valeur, comme des données financières ou des sauvegardes de serveurs. C'est ce qu'on appelle le « mouvement latéral ». Mais si le compte de ce commercial n'a jamais eu accès au système financier, l'attaquant est bloqué.

Il reste cantonné au service commercial. L'attaque est contenue, et les dégâts sont limités. Un rapport de 2025 a constaté que **41 % des attaques exploitaient des accès excessifs** pour se déplacer dans l'environnement et causer davantage de dommages. En veillant à ce que chacun dispose uniquement des accès nécessaires, vous retirez cette arme aux attaquants.

4. Avoir un processus clair lorsqu'une personne arrive ou quitte l'entreprise.

Cela résout le problème évoqué au début du chapitre. Vous avez besoin de deux checklists simples et non négociables : une pour l'arrivée d'une nouvelle personne, et une pour le départ d'une personne.

La checklist d'arrivée, ou processus d'onboarding, garantit qu'un nouveau collaborateur reçoit uniquement les accès nécessaires à son rôle spécifique, selon le principe du moindre privilège.

Il ne reçoit pas un identifiant générique identique à celui des autres ; ses accès sont adaptés à son poste dès le premier jour.

La checklist de départ, ou processus d'offboarding, est encore plus importante.

Dès que vous savez qu'un collaborateur quitte l'entreprise, ce processus doit démarrer immédiatement. Il doit s'agir d'une liste simple de tous les comptes auxquels cette personne a accès : sa messagerie, le lecteur réseau principal, ainsi que tous les outils SaaS utilisés par l'entreprise.

L'objectif est de couper tous les accès en quelques minutes ou, au minimum, en quelques heures.

Un processus d'offboarding rapide et complet est l'un des contrôles de sécurité les plus importants que vous puissiez avoir, car les anciens collaborateurs représentent un risque réel. Une étude a montré que **32 % des travailleurs reconnaissent avoir accédé au compte d'un ancien employeur** après leur départ.

Sans processus d'offboarding strict, vous vous retrouvez avec des « utilisateurs fantômes » : d'anciens comptes encore actifs appartenant à d'anciens collaborateurs.

Les recherches de 2025 montrent qu'une majorité d'organisations, souvent plus de 80 %, ont des comptes utilisateurs obsolètes ou dormants dans leurs systèmes, ce qui crée un risque de sécurité important. Par exemple, Microsoft indique que plus de 10 % des comptes Active Directory sont considérés comme obsolètes.

Ces comptes sont une mine d'or pour les attaquants. Ils sont souvent peu surveillés, et si un attaquant obtient le mot de passe de l'un d'eux, il peut accéder à votre réseau en ressemblant à un ancien collaborateur légitime, ce qui le rend beaucoup plus difficile à repérer.

Nettoyer ces anciens comptes et mettre en place un processus pour éviter que de nouveaux comptes fantômes ne se créent est essentiel.

ERREURS COURANTES À ÉVITER

Bien faire les choses importantes, c'est déjà la moitié du chemin. L'autre moitié consiste à éviter quelques erreurs fréquentes qui peuvent annuler tout votre travail. Elles semblent mineures, mais elles créent de grandes ouvertures pour un attaquant.

Partager des comptes « admin ».

C'est très courant, surtout dans les petites entreprises. Vous avez peut-être un identifiant « admin » principal pour votre serveur ou un logiciel clé, et toutes les personnes qui en ont besoin partagent le mot de passe par commodité. Cela arrive souvent avec des prestataires informatiques externes, lorsque toute leur équipe utilise un seul identifiant « admin ».

Le problème, c'est que vous ne savez pas qui a fait quoi.

Si quelqu'un commet une erreur et met un système hors service — ou pire, fait quelque chose de malveillant — vous avez plusieurs suspects, mais aucune preuve. Vous ne pouvez responsabiliser personne, car aucun journal ne montre précisément qui était connecté.

Quand quelque chose tourne mal, vous devez pouvoir consulter un journal et voir exactement quel compte personnel a effectué le changement. C'est la seule manière de comprendre rapidement ce qui s'est passé et de corriger le problème.

La règle doit être simple : une personne, un compte. Toujours. C'est particulièrement vrai pour tout compte capable de modifier vos systèmes.

Considérer la sensibilisation à la sécurité comme une action ponctuelle.

Personne n'apprend réellement quelque chose avec une vidéo de sécurité ennuyeuse d'une heure, imposée une fois par an.

Les collaborateurs cliquent jusqu'à la fin pour terminer, oublient tout une semaine plus tard, et cela ne change pas vraiment leur comportement.

Ce qui fonctionne, ce sont des rappels courts et réguliers. L'objectif est de construire, dans la durée, une habitude de prudence saine.

Les personnes jouent un rôle clé dans la grande majorité des violations ; ce n'est donc pas un sujet secondaire.

QUE DEMANDER À VOTRE PRESTATAIRE IT

En tant que dirigeant, votre rôle n'est pas de faire le travail technique, mais de responsabiliser votre équipe informatique ou votre prestataire IT. Pour cela, posez des questions simples, directes, et demandez des preuves.

Ces trois questions vous diront presque tout ce que vous devez savoir sur la manière dont vos collaborateurs et leurs accès sont gérés.

- **« Pouvez-vous me montrer un rapport qui prouve que 100 % de nos collaborateurs utilisent la MFA sur leur messagerie ? »** C'est une question fermée. N'acceptez pas « nous y travaillons » ou « la plupart des personnes l'utilisent ». Vous devez voir une preuve. La messagerie est la porte d'entrée de votre entreprise ; si un seul compte n'est pas protégé, le risque est considérable.

- **« Quel est notre processus formel lorsqu'un collaborateur quitte l'entreprise ? En combien de temps pouvez-vous garantir que tous ses accès seront coupés après notre notification ? »** La première partie oblige votre prestataire à disposer d'un vrai processus écrit, et pas seulement d'un plan informel du type « on s'en occupera ». La deuxième partie demande un engagement clair. La réponse attendue doit être un délai précis, par exemple « dans les 30 minutes suivant votre notification ».
- **« J'ai besoin de la liste de toutes les personnes qui disposent de droits administrateur sur notre réseau. Passons-la en revue ensemble la semaine prochaine. »** C'est l'une des revues les plus importantes que vous puissiez faire. Les droits administrateur sont les clés du royaume. Les personnes qui les détiennent peuvent tout faire, y compris créer de nouveaux utilisateurs, supprimer des données ou désactiver des contrôles de sécurité. Votre prestataire IT peut vous fournir la liste des personnes qui disposent de ces droits, mais vous seul, en tant que dirigeant, pouvez décider si elles en ont *encore* réellement besoin.

Appareils & sécurité des terminaux

Chaque ordinateur portable, ordinateur de bureau et téléphone utilisé pour le travail est un point d'entrée potentiel. S'ils ne sont pas sécurisés et maintenus à jour, ils créent des risques importants. Ce chapitre vous montre comment gérer tous les appareils qui accèdent aux données de votre entreprise. L'objectif est simple : chaque appareil doit être connu, sécurisé et à jour.

CE QU'IL FAUT FAIRE

Sécuriser vos appareils repose sur quelques habitudes de base. Si vous les appliquez correctement, vous éviterez la plupart des problèmes.

1. Tenir un inventaire à jour de tous les appareils.

C'est la base de tout le reste. Vous avez besoin d'une liste complète et actuelle de chaque ordinateur, ordinateur portable et téléphone utilisé pour votre entreprise. Cette liste doit être mise à jour régulièrement — c'est essentiel — et indiquer ce qui est connecté à votre entreprise à l'instant présent.

Vous ne pouvez pas protéger un appareil dont vous ignorez l'existence.

C'est également important si un ordinateur portable est perdu ou volé. Vous devez disposer d'une liste pour savoir ce qui manque, afin de pouvoir le verrouiller à distance ou effacer ses données. Lorsqu'un incident de sécurité survient, la première question est toujours : « Quel appareil est concerné ? » Sans inventaire, vous avancez à l'aveugle et perdez un temps précieux au moment de contenir une attaque.

- **Vous ne pouvez pas sécuriser ce que vous ne voyez pas.** Un inventaire constitue votre source de vérité unique sur ce que vous devez protéger.
- **C'est un système d'alerte précoce.** Un bon outil d'inventaire vous alerte lorsqu'un nouvel appareil inconnu se connecte à votre réseau, ou lorsqu'un appareil connu ne s'est plus manifesté et pourrait avoir disparu.
- **C'est indispensable pour répondre aux incidents.** Lorsqu'une attaque survient, identifier l'appareil qui a servi de point d'entrée est la première étape pour contenir le problème.

2. Imposer une configuration sécurisée pour chaque appareil.

Une fois que vous savez quels appareils vous possédez, assurez-vous que chacun respecte des paramètres de sécurité standards et obligatoires. Ce n'est pas facultatif. Tout appareil qui accède aux données de votre entreprise doit satisfaire à ces exigences minimales. Deux éléments sont non négociables :

Premièrement, chaque ordinateur portable et ordinateur de bureau doit avoir le **chiffrement complet du disque** activé. Cette fonctionnalité est intégrée aux systèmes d'exploitation modernes comme Windows et macOS. Elle rend toutes les données du disque illisibles sans le mot de passe. Si l'ordinateur portable d'un collaborateur est perdu ou volé, le chiffrement rend les données inutilisables pour le voleur. Sans chiffrement, il accède à vos listes clients, documents financiers et données de paie. Avec le chiffrement, il ne récupère qu'un appareil à revendre. Cela transforme une violation potentielle de données en simple désagrément lié au remplacement d'une machine.

Deuxièmement, vos collaborateurs ne devraient pas disposer de **droits administrateur locaux** sur leur ordinateur pour leur travail quotidien. Ces droits permettent d'installer des logiciels et de modifier des paramètres importants. S'ils sont compromis, un attaquant peut les utiliser pour désactiver les protections, installer des outils malveillants et se propager dans le réseau. Supprimer ces droits réduit fortement ce risque.

- **Les appareils perdus ou volés représentent un risque important.** Un rapport a montré que la perte ou le vol physique d'un appareil était un facteur dans **21 % des incidents de sécurité**. [21]Le chiffrement complet du disque est la solution simple.
- **Les attaquants exploitent les permissions excessives.** Un rapport 2025 de Palo Alto Networks a constaté que **41 % des attaques exploitaient des privilèges excessifs**[22], comme des droits administrateur, pour se déplacer dans un réseau et causer davantage de dégâts. Supprimer ces droits leur retire cet outil.

3. Utiliser une protection moderne des terminaux (EDR).

Les antivirus traditionnels, que vous utilisez probablement depuis des années, ne suffisent plus. Ils bloquent les menaces connues, mais restent aveugles face aux attaques modernes conçues pour ressembler à une activité normale, en utilisant les outils intégrés de l'ordinateur.

Vous avez besoin d'un outil moderne appelé **EDR**, pour *Endpoint Detection and Response*, c'est-à-dire détection et réponse sur les terminaux.

Un système EDR surveille activement vos ordinateurs à la recherche d'activités suspectes et de schémas d'attaque. Il peut détecter lorsqu'un programme apparemment normal, comme Microsoft Word, commence à se comporter de manière inhabituelle, par exemple en essayant de chiffrer des fichiers, puis vous alerter sur une menace potentielle.

La partie « réponse » de l'EDR est tout aussi essentielle. Lorsqu'il détecte un problème, un bon EDR peut automatiquement empêcher l'attaque de se propager. Par exemple, il peut mettre immédiatement en quarantaine un ordinateur infecté et le couper du reste du réseau. Cela transforme une crise potentielle à l'échelle de l'entreprise en un problème contenu sur un seul ordinateur portable. Mais l'outil ne représente que la moitié de la solution.

Quelqu'un doit surveiller les alertes et savoir comment agir lorsqu'un vrai problème est détecté.

- **La plupart des attaques commencent sur les terminaux** — l'ordinateur ou le téléphone d'un collaborateur —, avec des estimations généralement situées entre 60 % et 80 %. Cela en fait votre couche de défense la plus critique.

- **Les attaques modernes sont conçues pour être invisibles.** Les attaquants utilisent désormais des techniques « sans malware », en retournant les outils légitimes de votre ordinateur contre vous. Les antivirus traditionnels passent à côté ; un EDR, lui, surveille les comportements suspects et les détecte.
- **La rapidité de réaction est déterminante.** La différence entre un incident mineur et une violation majeure se joue souvent en quelques minutes. Un EDR capable d'isoler automatiquement un appareil vous fait gagner un temps critique pour réagir avant que la situation ne s'aggrave.

4. Mettre en place un processus régulier pour les mises à jour de sécurité.

C'est l'un des aspects les plus importants — et les plus souvent négligés — de la sécurité de base. Lorsqu'une entreprise comme Microsoft ou Google découvre une faille de sécurité dans son logiciel, elle publie un correctif, aussi appelé mise à jour de sécurité.

Dès que ce correctif est annoncé, une course commence. Vous et votre prestataire IT essayez de l'installer sur tous vos ordinateurs. En parallèle, les cybercriminels utilisent des outils automatisés pour scanner Internet à la recherche d'entreprises qui ne l'ont pas encore installé. Ils savent exactement à quoi ressemble la porte restée ouverte et disposent d'outils puissants pour la trouver.

C'est pourquoi vous avez besoin d'un processus simple et régulier pour installer les mises à jour. Les attaquants peuvent exploiter de nouvelles failles en quelques heures. Si vous attendez un mois, ou si vous le faites seulement quand cela vous arrange, vous leur laissez une grande fenêtre d'opportunité.

Votre processus n'a pas besoin d'être compliqué, mais il doit être régulier. Les mises à jour critiques des systèmes d'exploitation et des navigateurs web devraient être installées chaque semaine. Pour les vulnérabilités graves de type zero-day déjà exploitées activement, le correctif doit être appliqué dans un délai d'un à deux jours. Votre prestataire IT devrait gérer ce processus de manière automatisée, et vous devriez recevoir un rapport mensuel simple indiquant le pourcentage d'ordinateurs entièrement à jour.

- **Les attaques contre les logiciels non corrigés sont en forte hausse.** Selon le Verizon Data Breach Investigations Report 2025, les attaques exploitant des vulnérabilités logicielles comme première étape d'une violation représentent désormais 20 % des violations, soit une hausse de 34 % par rapport à l'année précédente.
- **Le nombre de nouvelles vulnérabilités est écrasant.** Rien qu'en 2024, près de **29'000 nouvelles vulnérabilités logicielles** ont été découvertes et signalées. [23]C'est un flux constant de nouvelles portes potentielles qu'il faut verrouiller.
- **L'écart entre le correctif et l'attaque est précisément là où vous êtes touché.** Une organisation moyenne met environ **55 à 67 jours pour installer les correctifs sur la moitié de ses vulnérabilités critiques**. Les attaquants peuvent exploiter ces mêmes failles en quelques heures. Un processus de gestion des correctifs régulier et rapide réduit cet écart dangereux.

ERREURS COURANTES À ÉVITER

Bien faire les choses importantes, c'est déjà la moitié du chemin. L'autre moitié consiste à éviter les erreurs courantes qui peuvent annuler tout votre travail. Elles semblent mineures, mais elles créent de grandes ouvertures pour les attaquants.

Laisser les collaborateurs être administrateurs de leur propre ordinateur.

Cette erreur fréquente est généralement motivée par la facilité. Lorsqu'un collaborateur dispose de « droits admin », il peut installer n'importe quel logiciel et modifier n'importe quel paramètre.

Le problème, c'est que s'il clique sur un lien malveillant, le malware installé obtient lui aussi ces droits administrateur. Il peut alors s'ancrer profondément dans l'ordinateur, désactiver la sécurité et se propager vers d'autres ordinateurs du réseau.

Comme mentionné dans un chapitre précédent, des rapports ont constaté que **41 % des attaques utilisaient exactement cette tactique**[24], en exploitant des permissions excessives pour se déplacer dans un réseau et causer davantage de dégâts.

Supprimer ces droits est une mesure simple, avec un impact énorme sur votre sécurité.

Ne pas avoir de plan pour les appareils personnels.

Il est courant que les collaborateurs utilisent leur téléphone ou leur ordinateur portable personnel pour travailler. C'est ce que l'on appelle le BYOD, pour *Bring Your Own Device*. Le problème, c'est que vous ne savez pas si cet appareil personnel est sécurisé. Est-il chiffré ? Dispose-t-il d'un mot de passe ? Ses logiciels sont-ils à jour ?

Si le téléphone personnel d'un collaborateur, avec accès à la messagerie de l'entreprise, est perdu ou volé, les données de votre entreprise sont exposées. Une étude a montré que **59 % des employeurs autorisent leurs collaborateurs à accéder aux applications de l'entreprise depuis des appareils personnels non gérés**.

Vous ne pouvez pas ignorer ce sujet. Si les collaborateurs utilisent des appareils personnels pour travailler, ces appareils doivent respecter vos exigences minimales de sécurité, comme un code de verrouillage et le chiffrement. Des outils simples permettent d'imposer ces règles sans accéder aux photos ou messages personnels.

QUE DEMANDER À VOTRE PRESTATAIRE IT

- **« Pouvez-vous me montrer un rapport qui liste tous les appareils accédant aux données de l'entreprise et confirme que 100 % d'entre eux sont chiffrés ? »** C'est une question fermée. N'acceptez pas « nous y travaillons » ou « la plupart le sont ». Ce rapport prouve que, si un ordinateur portable est volé, les données restent protégées.
- **« Quel est notre processus si l'ordinateur portable d'un collaborateur est perdu ou volé ? En combien de temps pouvez-vous garantir qu'il pourra être verrouillé ou effacé à distance ? »** La première partie les oblige à disposer d'un vrai processus documenté. La seconde demande un engagement clair. Vous devez savoir que vous pouvez contenir les dégâts d'un appareil perdu avant que quelqu'un tente d'y accéder.
- **« Quel outil de protection des terminaux utilisons-nous ? Les alertes sont-elles activement surveillées par une personne ? »** Cette question en deux parties est essentielle. Premièrement : quel outil ? Vous voulez entendre qu'il s'agit d'un EDR moderne, pas seulement d'un antivirus de base. Deuxièmement, et surtout : une personne surveille-t-elle les alertes ? Vous devez savoir que si une alerte arrive à 2 h du matin, quelqu'un la verra et agira.

Sécurité des e-mails, du web & des outils collaboratifs

Les e-mails, les navigateurs web et les outils collaboratifs comme Microsoft Teams, Slack ou Google Drive sont essentiels. Ils transportent des factures, des contrats, des données clients et des informations internes sensibles.

Malheureusement, cela en fait aussi des cibles privilégiées pour les cyberattaques.

Les arnaques de type compromission d'e-mail professionnel (BEC), où des criminels se font passer pour une personne de confiance afin de vous pousser à envoyer de l'argent, ont coûté aux entreprises près de **2,8 milliards de dollars en 2024 seulement**, avec une perte médiane de **50'000 dollars** par incident. [25]

Les attaques de phishing, souvent diffusées par e-mail, sont la menace la plus courante pour les petites entreprises et sont à l'origine de 68 % de toutes les violations de données. [26]

Ce chapitre vous montre comment protéger ces canaux de communication essentiels en mettant en place des filtres et garde-fous intelligents pour stopper les attaques et préserver la confidentialité de vos informations.

CE QU'IL FAUT FAIRE

Voici quatre habitudes et outils simples pour protéger les canaux de communication de votre entreprise. Si vous les mettez correctement en place, vous disposerez d'une défense solide contre les attaques les plus courantes.

1. Utiliser un outil avancé de sécurité e-mail.

Les filtres anti-spam et antivirus de base intégrés à Microsoft 365 ou Google Workspace sont utiles contre les courriers indésirables et les virus connus, mais ils ne sont pas conçus pour arrêter des attaques ciblées et bien préparées. Un outil avancé de sécurité e-mail ajoute une couche de protection supplémentaire pour détecter les menaces plus sophistiquées.

Ces outils font plus que les filtres de base. Lorsqu'un e-mail contient une pièce jointe, ils peuvent l'ouvrir dans un environnement isolé, appelé « sandbox », pour vérifier si elle est dangereuse. Si elle tente d'installer un logiciel malveillant, l'e-mail est bloqué avant d'arriver dans la boîte de réception.

Ils analysent aussi les liens dans les e-mails. Si un collaborateur clique, l'outil vérifie la destination en temps réel. Si le lien mène vers une fausse page de connexion ou un site contenant un logiciel malveillant, la connexion est bloquée et l'utilisateur est averti.

Les chiffres montrent à quel point cette protection est essentielle :

- L'e-mail est le principal vecteur de diffusion des logiciels malveillants, certaines études indiquant que jusqu'à **94 % de tous les malwares sont diffusés par e-mail**.[27]

2. Créer un processus non négociable pour les transactions financières.

Il s'agit d'une règle métier, pas d'une solution technologique, et c'est la mesure la plus importante pour éviter les fraudes par virement. Toute demande de changement de coordonnées bancaires d'un fournisseur, ou tout paiement inhabituel ou urgent, doit être vérifié par un appel téléphonique direct à un numéro que vous avez déjà dans vos dossiers pour cette personne.

Un e-mail ou un message texte ne suffit pas. Vous devez parler à une vraie personne par téléphone, en utilisant un numéro légitime que vous connaissez, et non un numéro indiqué dans l'e-mail de demande.

C'est crucial, car la technologie seule ne peut pas résoudre une défense qui repose sur un processus.

Cette fraude fonctionne en trompant une personne. Les attaquants exploitent la confiance que vous accordez à vos fournisseurs et à votre équipe. La seule façon de briser cette tromperie est de sortir du canal utilisé par l'attaquant, l'e-mail, et d'utiliser un autre canal : le téléphone.

Cette habitude simple, lorsqu'elle devient une règle non négociable de la culture de votre entreprise, bloque la forme la plus courante et la plus coûteuse de fraude par e-mail. Elle protège vos collaborateurs de situations difficiles et sécurise le compte bancaire de votre entreprise.

3. Filtrer le trafic web de votre équipe.

Voyez cela comme une ceinture de sécurité pour Internet. Un filtre web empêche vos collaborateurs d'accéder à des sites connus comme malveillants ou suspects. Avec le télétravail, cette protection doit être installée directement sur les ordinateurs portables, afin de les protéger partout.

Le filtre web agit comme un filet de sécurité. Beaucoup d'attaques commencent par un mauvais lien dans un e-mail. Si ce lien mène vers un site malveillant ou une fausse page Microsoft 365, le filtre bloque l'accès avant que l'ordinateur ne soit infecté ou que l'utilisateur ne saisisse son mot de passe.

Il protège vos collaborateurs contre des erreurs commises en une fraction de seconde, qui peuvent autrement provoquer des catastrophes à l'échelle de l'entreprise. C'est une barrière automatique qui les maintient du bon côté de la route.

Les chiffres montrent pourquoi ce filet de sécurité est nécessaire :

- Le Verizon Data Breach Investigations Report 2024 montre que **68 % de toutes les violations impliquent un facteur humain non malveillant**, souvent à partir d'un collaborateur qui clique sur un lien de phishing.
- Lorsque les personnes se font piéger par ces arnaques, cela arrive incroyablement vite. Le temps médian avant qu'un utilisateur clique sur un lien de phishing est de **moins de 25 secondes**. Ce n'est pas assez pour s'arrêter et réfléchir, d'où la nécessité d'un outil automatisé.[28]
- Le phishing est le vecteur d'attaque le plus courant pour les petites entreprises, **61 % des PME déclarant qu'il s'agissait du type d'attaque le plus fréquent** observé l'année dernière.[29]

4. Définir des paramètres sécurisés par défaut pour le partage de fichiers.

Les outils collaboratifs comme Microsoft Teams, SharePoint et Google Drive sont très utiles, mais ils facilitent parfois trop le partage. L'option la plus risquée est le « lien public » ou « partager avec toute personne ». Elle crée un lien accessible à n'importe qui sur Internet, sans mot de passe ni connexion.

Les données sensibles fuient souvent depuis ces plateformes lorsqu'un collaborateur crée accidentellement l'un de ces liens publics. Il essaie peut-être de partager un dossier avec un seul client, mais, dans la précipitation, il choisit la mauvaise option. Le dossier, qui peut contenir des contrats sensibles ou des informations financières, devient alors public. Le lien peut être transféré, publié en ligne et parfois même trouvé par des moteurs de recherche.

C'est pourquoi il est essentiel de configurer ces outils afin que tout nouveau fichier ou dossier soit **privé par défaut**.

Le partage doit être un acte volontaire, pas le réglage par défaut. Faites en sorte que l'option sécurisée soit la plus simple. Un collaborateur devrait devoir effectuer des étapes supplémentaires pour partager quelque chose publiquement, afin de l'obliger à réfléchir à son action. Configurer le mode privé par défaut évite toute cette catégorie de violations accidentelles de données.

Les données montrent à quel point les outils cloud mal configurés sont devenus répandus :

Les intrusions dans le cloud ont **augmenté de 75 %** ces dernières années, en grande partie à cause de mauvaises configurations simples, comme des données exposées publiquement.[30]
Un autre rapport 2025 a constaté que **99 % des organisations ont des données exposées** dans leurs environnements cloud, souvent à cause de ces mauvaises configurations.[31]

ERREURS COURANTES À ÉVITER

Comme nous l'avons vu précédemment, bien faire les choses importantes représente déjà la moitié du travail ; l'autre moitié consiste à éviter les erreurs courantes qui peuvent annuler tous vos efforts. Ces éléments, qui semblent mineurs, créent en réalité de grandes ouvertures pour les attaquants.

Penser que la sécurité par défaut de Microsoft 365 ou Google suffit.

Beaucoup de personnes pensent que la sécurité de base incluse avec Microsoft 365 ou Google est suffisante. Ces filtres par défaut ne sont souvent pas assez efficaces pour arrêter des attaques ciblées et bien préparées, comme les fausses factures dont nous avons parlé. Les attaquants savent ce que ces filtres recherchent et conçoivent leurs attaques pour les contourner. Vous avez besoin d'une couche de sécurité supplémentaire, spécifiquement conçue pour repérer ces menaces plus avancées et ciblées.

Faire confiance à l'e-mail dès qu'il est question d'argent.

C'est une erreur majeure. L'e-mail n'a jamais été conçu comme un moyen sécurisé pour transférer de l'argent. Les attaquants peuvent facilement faire croire qu'un e-mail provient d'une personne de confiance. Ils peuvent imiter le nom de l'expéditeur et parfois même l'adresse e-mail elle-même, ce qui rend la fraude très difficile à repérer. Dès qu'il est question d'argent, vous devez partir du principe que l'e-mail pourrait être faux.

Penser que la formation à la sécurité suffit à stopper le phishing.

La sensibilisation à la sécurité est importante ; vous devez absolument apprendre à votre équipe ce qu'elle doit surveiller.

Cependant, vous ne pouvez pas attendre de la formation seule qu'elle règle le problème. Les gens sont occupés, distraits et commettent des erreurs. Les attaquants conçoivent leurs arnaques précisément pour exploiter ces moments d'inattention. Il suffit qu'une personne fasse une seule erreur, un après-midi chargé, pour qu'un attaquant entre.

C'est pourquoi vous avez besoin des contrôles techniques dont nous avons parlé, comme un filtre e-mail avancé et un filtre web. Ils constituent le filet de sécurité lorsque, inévitablement, une personne commet une erreur.

QUE DEMANDER À VOTRE PRESTATAIRE IT

Votre rôle en tant que dirigeant n'est pas de faire le travail technique, mais vous devez responsabiliser votre équipe informatique ou votre prestataire IT. Pour cela, posez des questions simples et directes, qui exigent des preuves — pas seulement des promesses.

- **« Quel outil précis utilisons-nous pour la sécurité e-mail, au-delà du filtre de base intégré ? Comment nous protège-t-il si quelqu'un clique sur un mauvais lien ? »** S'ils ne peuvent pas expliquer simplement comment l'outil vous protège contre un lien malveillant, c'est qu'il ne remplit pas sa fonction la plus importante.
- **« Pouvez-vous configurer notre système e-mail pour ajouter automatiquement un bandeau d'avertissement en haut de tous les e-mails provenant de l'extérieur de l'entreprise ? »** C'est un contrôle simple, mais extrêmement efficace. Un bandeau indiquant « **E-MAIL EXTERNE** » en haut d'un message rappelle constamment à votre équipe de rester un peu plus prudente. C'est particulièrement utile pour repérer les arnaques où un attaquant essaie de se faire passer pour vous ou pour un autre membre de la direction. C'est un petit rappel qui peut éviter une très grosse erreur.
- **« Les paramètres de partage de fichiers de notre entreprise dans Teams/Google Drive sont-ils réglés sur "privé par défaut" ? Pouvez-vous me montrer la règle qui l'impose ? »** Cette question vérifie si vous êtes protégé contre les fuites accidentelles dues au partage public. La réponse devrait être simplement « oui ». La seconde partie — « pouvez-vous me montrer la règle » — permet d'obtenir la preuve. Ils devraient pouvoir vous montrer une capture du paramètre d'administration qui applique cette règle à toute l'entreprise. Cela confirme qu'il s'agit d'une règle réelle et imposée, pas seulement d'une recommandation.

Protection des données

Perdre vos données lors d'une cyberattaque ou d'une panne peut mettre votre activité en danger. Ce chapitre vous montre comment les garder en sécurité et disponibles.

Nous allons couvrir deux aspects essentiels : la confidentialité, c'est-à-dire le fait que seules les personnes autorisées puissent consulter vos données, et la disponibilité, c'est-à-dire votre capacité à y accéder en tout temps.

CE QU'IL FAUT FAIRE

Protéger vos données repose sur quatre habitudes de base. Si vous les appliquez correctement, vous disposerez d'un filet de sécurité solide pour les données de votre entreprise.

1. Suivre la règle de sauvegarde 3-2-1.

Cette stratégie simple et éprouvée vous aide à récupérer après toute perte de données.

- Conservez au moins **3** copies de vos données : vos données actives plus deux sauvegardes.
- Stockez ces copies sur **2** types de supports différents, par exemple votre serveur et un appareil de sauvegarde séparé, ou un appareil local et un service cloud.
- Gardez **1** de ces copies hors site et complètement séparée de votre réseau principal.

Cette règle vous protège contre un événement unique qui détruirait tout. Par exemple, si un incendie détruit vos bureaux, votre sauvegarde cloud reste en sécurité.

Aujourd'hui, l'élément le plus important est la **copie isolée**. C'est votre meilleure défense contre les rançongiciels. Les attaquants ciblent souvent les sauvegardes avant de verrouiller les fichiers principaux.

Une copie isolée est une copie qu'un attaquant ne peut pas atteindre depuis votre réseau principal. Il existe deux façons principales d'y parvenir : une sauvegarde « air-gapped » ou une sauvegarde « immuable ».

Une sauvegarde « air-gapped » est physiquement déconnectée du réseau, comme un disque dur externe que vous branchez, utilisez, puis débranchez et stockez en lieu sûr.

Une sauvegarde immuable, proposée par de nombreux services de sauvegarde cloud, empêche toute personne — vous y compris — de modifier ou supprimer une sauvegarde pendant une période définie. Cela protège contre les attaques par rançongiciel qui se propagent aux supports de sauvegarde connectés, comme dans l'exemple évoqué au début.

- **Les attaquants ciblent vos sauvegardes.** Un rapport 2024 a constaté que, dans **94 % des attaques par rançongiciel**, les attaquants avaient tenté de compromettre les sauvegardes de la victime.[32]

94%

des attaques par rançongiciel tentent d'abord de détruire vos sauvegardes

- **Des sauvegardes compromises ralentissent la récupération.** Pour les entreprises dont les sauvegardes ont été compromises, seules **22 % ont récupéré en une semaine ou moins**. [33]
- **Les échecs de sauvegarde sont fréquents.** Une étude a constaté que les erreurs de sauvegarde, y compris les sauvegardes corrompues par des rançongiciels, contribuaient à environ **un tiers de tous les incidents de perte de données**.[34]

2. Tester régulièrement la restauration de vos sauvegardes.

Une sauvegarde n'a de valeur que si vous pouvez réellement l'utiliser. Le message « Succès » affiché par votre logiciel de sauvegarde ne signifie pas que vous pouvez remettre votre entreprise en route. Il indique seulement que des fichiers ont été copiés. Vous ne saurez pas si ces fichiers sont exploitables, ni si vous disposez de tout ce qu'il faut, tant que vous n'aurez pas testé une restauration.

Un test de restauration est un exercice planifié durant lequel vous récupérez des fichiers, des dossiers, voire des systèmes entiers à partir de votre sauvegarde. Vous n'avez pas besoin de restaurer toute l'entreprise à chaque fois, mais vous devez tester régulièrement.

Ces tests vous permettent de détecter les problèmes lorsque les enjeux sont faibles. Vous voulez découvrir qu'un dossier critique manque, qu'une base de données est corrompue ou qu'une clé de licence logicielle indispensable est introuvable pendant un test, pas au beau milieu d'une véritable attaque par rançongiciel.

En plus, ces exercices développent les réflexes de votre équipe. En situation de crise réelle, elle suivra une checklist déjà pratiquée au lieu d'essayer de tout comprendre pour la première fois.

- **Des sauvegardes non testées peuvent entraîner une perte définitive de données.** Même si ce chiffre n'est pas validé à 100 %, une étude a constaté que près de **60 % des petites entreprises qui perdent leurs données ferment dans les six mois**.
- **Beaucoup d'entreprises ne testent pas.** Le rapport 2025 Unitrends State of Backup and Recovery indique que 25 % des organisations testent leurs plans de reprise après sinistre une fois par an ou moins.[35]

3. Savoir où se trouvent vos données les plus importantes.

Vous ne pouvez pas protéger vos données les plus importantes si vous ne savez pas où elles se trouvent. Comme pour vos actifs physiques, vous devez savoir où sont vos « joyaux numériques ».

Avec le temps, les données se dispersent. Une proposition commerciale critique peut être enregistrée sur le bureau d'un collaborateur au lieu d'un lecteur partagé. Un tableau financier important peut se retrouver dans un dossier Dropbox personnel. Une ancienne liste clients peut être stockée sur un ordinateur portable de réserve dans une armoire. Lorsque les données sont éparpillées, il devient difficile de les protéger.

Les fichiers stockés sur des bureaux d'ordinateur ou dans des dossiers cloud personnels ne sont pas sauvegardés par le système de votre entreprise et ne bénéficient pas du même niveau de sécurité que les fichiers placés sur votre serveur principal.

Posez-vous les questions suivantes :

- Où se trouvent nos fichiers comptables ?
- Où se trouve notre base clients principale ?
- Où sont stockés les dossiers RH de nos collaborateurs ?
- Où conservons-nous nos contrats signés et notre propriété intellectuelle ?

Une fois que vous savez où ces données critiques doivent se trouver, vous pouvez les protéger. Vous pouvez confirmer que cet emplacement est sauvegardé et appliquer des contrôles de sécurité plus stricts, en limitant l'accès uniquement aux personnes qui en ont besoin. Cela vous permet de concentrer vos efforts sur ce qui compte vraiment.

- **La dispersion des données est un problème important.** Une étude a constaté que, dans plus de **64 % des entreprises de services financiers, plus de 1'000 fichiers sensibles étaient accessibles à tous les collaborateurs**, ce qui montre à quel point les données se dispersent facilement et à quel point les accès sont souvent trop larges.
- **La plupart des entreprises suivent mal leurs données.** Une autre étude a constaté que **seule une entreprise sur dix** disposait d'un bon système d'étiquetage des fichiers, ce qui rend presque impossible le suivi des données sensibles.[36]

4. Chiffrer les appareils qui stockent des données de l'entreprise.

Vous devez activer le chiffrement intégré sur tous les ordinateurs portables de l'entreprise. Cette fonctionnalité existe déjà ; il faut simplement l'activer pour tout le monde.

Le chiffrement brouille toutes les données du disque dur et les rend illisibles sans le mot de passe. C'est essentiel, car les ordinateurs portables sont souvent perdus ou volés. Si un collaborateur oublie son ordinateur dans un café ou se le fait voler dans sa voiture, un appareil non chiffré donne au voleur un accès complet à vos listes clients, documents financiers, informations de paie et mots de passe enregistrés. Il s'agit alors d'une véritable violation de données.

Avec le chiffrement, un ordinateur portable volé n'est plus qu'un appareil matériel. Les données restent en sécurité. Cela transforme une catastrophe potentielle, que vous devriez signaler à vos clients et à votre assurance, en simple désagrément lié au remplacement d'un ordinateur.

- **La perte ou le vol physique d'un appareil représente un risque majeur.** Un rapport a montré que cela constituait un facteur dans **21 % des incidents de sécurité**[37]. Le chiffrement répond directement à ce problème courant.
- **La plupart des petites entreprises ne chiffrent pas leurs données.** Malgré son efficacité et sa simplicité d'utilisation, une enquête a constaté que **seules 17 % des petites entreprises chiffrent leurs données**. Cette étape simple vous place déjà largement en avance.

ERREURS COURANTES À ÉVITER

Bien faire les choses importantes est essentiel, mais éviter quelques erreurs courantes l'est tout autant. Ces erreurs, qui semblent mineures, peuvent créer de grandes failles de sécurité.

Garder votre seule copie de sauvegarde connectée au réseau principal.

Les hackers sont malins. Ils ciblent et détruisent souvent les sauvegardes en premier, puis lancent le rançongiciel, vous laissant sans aucun moyen de récupérer vos données.

Votre seule copie réellement sûre doit être isolée de votre réseau principal, soit physiquement déconnectée — « air-gapped » —, soit protégée dans le cloud de façon à ne pas pouvoir être modifiée — immuable.

Oublier de sauvegarder des données clés.

Cela arrive souvent lorsque vous ne savez pas où se trouvent vos données importantes. Votre serveur principal est peut-être bien sauvegardé, mais un excellent commercial peut enregistrer des propositions importantes sur son bureau.

Votre équipe financière peut avoir un tableau critique dans un dossier OneDrive personnel. Ces données ne sont pas sauvegardées par le système de votre entreprise. Si cet ordinateur portable tombe en panne ou si le collaborateur quitte l'entreprise, les données disparaissent. Vous devez identifier vos données « joyaux de la couronne » et vous assurer qu'elles sont enregistrées dans des emplacements centralisés et gérés, afin qu'elles soient correctement sauvegardées.

Confondre un service de synchronisation cloud avec une vraie sauvegarde.

Beaucoup de personnes pensent que, parce que leurs fichiers se trouvent dans Dropbox, Google Drive ou OneDrive, ils sont sauvegardés. C'est faux. Ce sont des services de synchronisation de fichiers, très utiles pour collaborer, mais ce ne sont pas des sauvegardes.

Si vous supprimez accidentellement un fichier, il est supprimé dans le cloud. Si un rançongiciel chiffre vos fichiers, ces fichiers chiffrés sont synchronisés vers le cloud et écrasent vos bonnes copies.

Une vraie sauvegarde est une copie séparée de vos données à un instant donné, protégée contre ce type de modifications. Un service de synchronisation n'est pas conçu pour servir de filet de sécurité.

QUE DEMANDER À VOTRE PRESTATAIRE IT

Ces trois questions vous diront presque tout ce que vous devez savoir sur votre protection des données.

- **« Quand avons-nous effectué notre dernier test complet de restauration ? Combien de temps a-t-il pris, et puis-je voir le rapport ? »** C'est une question directe de responsabilisation. N'acceptez pas « nous faisons des sauvegardes chaque nuit ». Ce que vous devez connaître, c'est la *restauration*. La réponse devrait être précise, par exemple : « Nous avons fait un test le trimestre dernier. Nous avons restauré le serveur de fichiers principal. Cela a pris quatre heures, et voici le résumé d'une page des résultats. » Cela prouve que les tests sont réalisés et vous donne une idée concrète de la durée d'interruption en cas de crise.
- **« Montrez-moi comment notre copie de sauvegarde hors site est protégée contre une attaque par rançongiciel. Est-elle hors ligne ou "immuable" ? »** Cette question vise la plus grande menace pour votre plan de récupération. Si elle est hors ligne, demandez-leur de décrire le processus physique. Si elle est immuable, demandez-leur de vous montrer le paramètre dans le service de sauvegarde cloud qui confirme qu'elle ne peut pas être supprimée. Cela confirme que vous disposez d'une copie sûre qu'un attaquant ne peut pas détruire.
- **« Pouvez-vous me fournir la liste des emplacements de données critiques qui sont sauvegardés, afin de confirmer que nous n'avons rien oublié d'important ? »** Cette question répond au problème de « savoir où se trouvent vos données ». Donnez à votre prestataire IT la liste de vos emplacements de données les plus importants — dossier comptable, base clients, lecteur des contrats. Il devrait vous remettre un rapport ou une capture d'écran montrant que ces emplacements précis sont inclus dans la tâche de sauvegarde.

Bases des réseaux & du cloud

Le réseau de votre entreprise est comme son système nerveux. Il relie tout : les ordinateurs portables de vos collaborateurs, vos serveurs et vos services cloud. Si un attaquant compromet ce réseau, l'ensemble de votre entreprise peut être exposé.

Ce chapitre vous montre comment mettre en place un « plan d'étage » sécurisé pour votre réseau et vos services cloud, avec des zones séparées et protégées. Cela empêche un problème dans une zone de se propager à toute l'entreprise, tout en gardant vos données privées et protégées.

CE QU'IL FAUT FAIRE

Pour gérer votre réseau et vos services cloud de manière sécurisée, concentrez-vous sur ces trois habitudes. Elles permettent d'éviter la plupart des problèmes.

1. Segmentez votre réseau.

Imaginez votre réseau comme un immeuble de bureaux. Vous ne laisseriez pas un visiteur arrivé à la réception se promener librement dans votre salle serveur. La même logique s'applique à votre réseau informatique. La

segmentation réseau consiste à installer des murs à l'intérieur de votre réseau pour créer des zones séparées et sécurisées.

Au minimum, créez un réseau Wi-Fi séparé pour les invités. Ce réseau invité ne doit permettre que l'accès à Internet et doit être complètement isolé de votre réseau principal d'entreprise. Cette mesure simple empêche les menaces, comme un malware présent sur l'ordinateur portable d'un visiteur, d'atteindre les systèmes de votre entreprise.

Pour une sécurité encore meilleure, utilisez trois zones séparées :

- Un réseau principal pour les ordinateurs de confiance, gérés par l'entreprise.
- Un réseau invité pour les visiteurs, avec accès à Internet uniquement.
- Un troisième réseau pour les appareils moins sécurisés, comme les téléviseurs connectés, les caméras de sécurité ou les téléphones personnels des collaborateurs.

Cette segmentation contient les menaces. Si un attaquant compromet votre téléviseur connecté, il ne peut pas l'utiliser pour attaquer votre serveur principal. Elle limite les dégâts. Sans ces murs internes — ce que l'on appelle un « réseau plat » — les attaquants peuvent se déplacer librement, ce que l'on appelle le « mouvement latéral », pour trouver vos données les plus précieuses. La segmentation rend cela beaucoup plus difficile.

- **Les attaquants comptent sur leur capacité à se déplacer.** Un rapport 2025 a constaté que **41 % des attaques utilisaient des privilèges excessifs pour effectuer des mouvements latéraux** et causer davantage de dégâts. [38]La segmentation bloque directement cette tactique.
- **Elle vous protège contre ce que vous ne contrôlez pas.** Vous ne pouvez pas contrôler la sécurité des ordinateurs portables des visiteurs ni des téléphones personnels des collaborateurs. La segmentation leur donne un accès Internet sans exposer votre entreprise aux risques liés à leurs appareils.

2. Sécuriser vos accès à distance.

Avec l'augmentation du télétravail, la manière dont les collaborateurs se connectent aux systèmes de l'entreprise devient une cible majeure pour les attaquants. Vous devez verrouiller ces portes numériques.

N'exposez jamais directement à Internet des outils comme le protocole Remote Desktop (RDP). RDP est un outil intégré à Windows qui permet de contrôler un ordinateur à distance. L'exposer à Internet revient à afficher une pancarte « piratez-moi » devant votre entreprise.

Les groupes de rançongiciels utilisent des outils automatisés pour scanner Internet 24 h/24 et 7 j/7 à la recherche de cette erreur.

Ils trouveront votre serveur RDP ouvert et utiliseront d'autres outils automatisés pour deviner le mot de passe. S'ils y parviennent, ils prennent le contrôle complet de votre serveur, et une attaque par rançongiciel peut suivre en quelques heures.

Tous les accès à distance des collaborateurs doivent passer par une passerelle moderne et sécurisée qui exige l'authentification multifacteur (MFA). Ainsi, même si un attaquant vole le mot de passe d'un collaborateur, il ne peut pas se connecter sans le téléphone de celui-ci pour approuver l'accès.

- **C'est une cible principale des rançongiciels.** Microsoft rappelle régulièrement que le RDP non protégé est l'une des principales méthodes utilisées par les groupes de rançongiciels pour entrer dans les entreprises.
- **C'est un point d'entrée très fréquent.** Des études montrent que les services d'accès à distance exposés constituent le point d'entrée initial de **plus de 50 % des déploiements de rançongiciels**.[39]

3. Configurer les services cloud en « privé par défaut ».

Lorsque vous utilisez des services cloud comme Microsoft 365, Google Drive ou Dropbox, vous devez comprendre vos responsabilités en matière de sécurité.

Le fournisseur — Microsoft, Google, Amazon — sécurise le cloud lui-même : les centres de données physiques, les serveurs et les réseaux principaux. Vous êtes responsable de la sécurité dans le cloud : la configuration, les accès et la protection de vos données.

La plus grande erreur cloud tient souvent à une simple erreur humaine, comme beaucoup de choses en cybersécurité.

Un collaborateur, pressé de partager un dossier avec un client, clique sur « partager avec toute personne » ou « lien public ». Il vient de rendre ce dossier, et tout ce qu'il contient, public. Toute personne disposant du lien peut y accéder sans mot de passe ni connexion.

C'est pourquoi vous devez fixer une règle : tout nouvel espace de stockage cloud — nouveau dossier SharePoint, nouveau site, nouveau « bucket » Amazon S3 — doit être créé avec les paramètres les plus sécurisés et privés.

L'accès ne doit jamais être ouvert par défaut. Vous devez accorder les accès volontairement, personne par personne. La méthode sécurisée doit être la plus simple ; la méthode risquée doit exiger des étapes et validations supplémentaires.

Cette erreur est la cause la plus fréquente des grandes violations de données dans le cloud. Un collaborateur ne cherche pas à exposer votre liste clients ou vos prévisions financières, mais si le réglage par défaut est « public », cela peut arriver très facilement par accident. Définir le mode « privé » par défaut évite ce type de fuite. C'est un changement simple qui agit comme un puissant filet de sécurité contre les erreurs humaines du quotidien.

- **Les mauvaises configurations cloud sont un problème majeur.** Un rapport 2025 de Palo Alto Networks a constaté que **40 % des incidents cloud provenaient d'actifs non surveillés et de shadow IT**, incluant souvent des dossiers mal configurés.
- **La plupart des violations impliquent désormais le cloud.** Les données montrent clairement que le risque se situe ici. Un rapport IBM 2025 a constaté que **72 % des violations de données impliquaient des données stockées dans le cloud**.

ERREURS COURANTES À ÉVITER

Bien faire les choses importantes est essentiel, mais éviter ces erreurs courantes l'est tout autant. Elles peuvent sembler mineures, mais elles créent de grandes ouvertures pour les attaquants.

Penser que votre fournisseur cloud gère toute votre sécurité.

C'est un malentendu coûteux. Lorsque vous utilisez des services comme Microsoft 365 ou Google Workspace, vous êtes dans un « modèle de responsabilité partagée ». Le fournisseur sécurise le cloud lui-même — centres de données physiques, serveurs et réseaux principaux.

Vous êtes responsable de la sécurité dans le cloud — contrôle des accès, permissions et partage des données. Le fournisseur cloud vous met à disposition les outils de sécurité, mais c'est à vous de les utiliser correctement.

Utiliser un mot de passe partagé pour votre réseau Wi-Fi principal.

C'est une autre erreur motivée par la facilité, mais elle crée de gros risques. Si vous avez un seul mot de passe pour le Wi-Fi principal de l'entreprise et que vous le donnez à chaque nouveau collaborateur, que se passe-t-il lorsqu'un collaborateur quitte l'entreprise ? Pour lui retirer l'accès au réseau, vous devez changer le mot de passe, puis mettre à jour chaque appareil dans les bureaux.

C'est une énorme contrainte, donc cela se fait rarement. Cela signifie qu'un ancien collaborateur pourrait potentiellement se connecter à votre réseau interne des mois, voire des années plus tard. Les systèmes Wi-Fi modernes évitent ce problème en permettant à chaque collaborateur de se connecter avec son propre identifiant et mot de passe, les mêmes que pour son ordinateur. Lorsqu'il quitte l'entreprise, vous désactivez simplement son compte, et son accès Wi-Fi disparaît.

QUE DEMANDER À VOTRE PRESTATAIRE IT

Ces trois questions vous diront presque tout ce que vous devez savoir sur la qualité de gestion de votre réseau et de vos services cloud.

- **« Notre réseau Wi-Fi invité est-il complètement séparé de notre réseau principal d'entreprise ? Pouvez-vous me montrer la configuration qui le prouve ? »** C'est une question fermée. Votre prestataire devrait pouvoir vous montrer une capture des règles de pare-feu ou de la configuration réseau qui bloque clairement le trafic du réseau « Invité » vers le réseau « Interne ». C'est une confirmation visuelle simple que le mur est bien en place.
- **« Avons-nous des services, en particulier Remote Desktop (RDP), exposés directement à Internet ? J'ai besoin d'une confirmation que tous les accès à distance passent par une passerelle sécurisée et gérée. »** Cette question confirme que la porte la plus dangereuse a été fermée et remplacée par une solution sécurisée exigeant l'authentification multifacteur.
- **« Quel est notre processus pour garantir qu'un nouveau dossier ou site SharePoint est créé par défaut avec des paramètres privés, et non publics ? »** Cette question vérifie si vous êtes protégé contre les fuites accidentelles de données dans le cloud. Votre prestataire IT devrait pouvoir vous montrer le paramètre d'administration dans Microsoft 365 ou Google Workspace qui applique cette règle à tous les utilisateurs de l'entreprise. Cela ne devrait pas être une simple recommandation aux collaborateurs ; ce doit être un contrôle technique qui fait de l'option sécurisée le réglage par défaut. Cela prouve qu'il gère votre environnement cloud de manière proactive, et pas seulement en réaction aux problèmes.

Risque fournisseurs & tiers

Toutes les entreprises dépendent de partenaires et de fournisseurs externes pour fonctionner. Chacune de ces connexions représente un point d'entrée potentiel pour des cyberattaquants, même si votre propre sécurité est solide.

Un problème chez l'un de vos fournisseurs peut rapidement devenir une catastrophe pour votre entreprise.

Ce chapitre vous montre comment gérer ces risques. L'objectif est de comprendre les risques apportés par chaque partenaire, puis de mettre en place des moyens simples pour vérifier leur fiabilité et limiter leurs accès à ce qui est strictement nécessaire.

CE QU'IL FAUT FAIRE

Vous devez développer quatre habitudes de base pour gérer les risques liés à vos partenaires. Si vous les appliquez correctement, vous disposerez d'une approche solide et raisonnable pour protéger votre entreprise contre les risques de sa chaîne d'approvisionnement.

1. Classer vos fournisseurs par niveau de risque.

Commencez par identifier tous vos fournisseurs. En sécurité, un « fournisseur » ou « tiers » désigne toute personne, entreprise ou solution logicielle qui se connecte à votre entreprise ou traite vos données. Cela inclut votre prestataire IT, votre prestataire de paie, votre logiciel comptable, votre CRM commercial et même votre outil de newsletter marketing.

Une fois cette liste établie, classez-les. Vous ne pouvez pas traiter votre fournisseur de café comme l'entreprise qui a accès à votre serveur. Ce n'est ni efficace ni nécessaire. L'objectif est de les regrouper simplement afin de concentrer votre attention là où le risque est le plus élevé.

Pour cela, posez deux questions pour chaque fournisseur :

- À quel point est-il critique pour vos opérations quotidiennes ? S'il cessait de fonctionner pendant une journée, serait-ce un problème mineur ou majeur ?
- Quelle est la sensibilité des données que vous lui confiez ? Reçoit-il seulement votre adresse publique, ou traite-t-il les données personnelles de vos collaborateurs et les données financières de votre entreprise ?

Cela regroupera naturellement vos fournisseurs.

Vos fournisseurs « à haut risque » sont ceux qui sont critiques pour votre activité et qui traitent vos données les plus sensibles. Cette liste doit rester courte. Elle inclut généralement votre prestataire IT, votre prestataire de paie et peut-être votre principal logiciel comptable ou opérationnel. Ce sont les partenaires qui, en cas de problème, pourraient mettre votre entreprise à l'arrêt. Ce sont les seuls pour lesquels vous devez consacrer un temps significatif. Tous les autres fournisseurs relèvent d'une catégorie de risque plus faible.

2. Poser des questions de sécurité de base avant de signer un contrat.

Une fois que vous savez qui sont vos fournisseurs à haut risque, parlez-leur de sécurité.

Pour tout nouveau fournisseur à haut risque, utilisez une courte liste de questions simples à poser avant de signer le contrat. Vous cherchez simplement à confirmer qu'il prend la sécurité aussi au sérieux que vous.

Voici quelques bonnes questions directes à poser :

- Utilisent-ils l'authentification multifacteur (MFA) pour tous les collaborateurs qui accèdent à vos données ?
- Ont-ils un processus régulier pour installer les mises à jour de sécurité sur leurs systèmes ?
- Comment protègent-ils vos données lorsqu'ils les stockent ? Sont-elles chiffrées ?
- Que se passe-t-il s'ils rencontrent un problème de sécurité ? Dans quel délai vous en informeront-ils ?

C’est très important, car un problème chez votre fournisseur peut rapidement devenir votre problème.

- Les données montrent que **15 % de toutes les violations en 2024 impliquaient un tiers**, soit une **hausse de 68 %** par rapport à l’année précédente.[40]
- Une autre étude a constaté que **59 % des entreprises ont subi une violation de données causée par l’un de leurs fournisseurs tiers**.[41]

3. Donner aux fournisseurs un accès limité et limité dans le temps.

Vous devez appliquer strictement cette règle. Lorsque vous donnez accès à vos systèmes à une personne ou une entreprise externe, faites-le de manière très précise.

Premièrement, **n’utilisez jamais de comptes partagés.** Il est courant qu’une entreprise crée un seul identifiant, par exemple « IT_Vendor_Admin », puis donne le mot de passe à toute l’équipe de support IT du fournisseur. C’est une grosse erreur. Si quelque chose tourne mal — un fichier supprimé, un réglage modifié qui fait planter votre système — vous ne savez pas qui l’a fait.

Vous savez seulement que cela vient de quelqu’un chez le fournisseur. Il n’y a donc aucune responsabilité claire. La règle doit être simple : chaque personne externe qui a besoin d’accéder à vos systèmes reçoit son propre compte nominatif et unique. Ainsi, si « john.smith@itvendor.com » effectue une modification, vous savez exactement de qui il s’agit.

Deuxièmement, ce compte doit être **limité à ce qui est nécessaire pour son travail**. C’est le principe du moindre privilège que nous avons déjà évoqué, mais il est encore plus important pour les fournisseurs externes. Si vous avez mandaté une entreprise pour travailler sur votre site web, son compte doit uniquement donner accès au serveur du site, pas à votre serveur de fichiers principal ni à votre logiciel comptable. C’est ainsi que vous limitez les dégâts si le compte de ce fournisseur est compromis.

Enfin, chaque compte fournisseur doit avoir une **date d’expiration définie**. Si vous engagez un prestataire pour un projet de trois mois, son compte doit se désactiver automatiquement le dernier jour du projet. C’est essentiel, car il est facile d’oublier de supprimer les accès d’un fournisseur une fois son travail terminé. Ces anciens comptes oubliés, souvent appelés « utilisateurs fantômes », représentent un risque de sécurité majeur.

C’est important parce que cela ferme l’une des failles de sécurité les plus courantes en entreprise. Lorsqu’un projet se termine, personne ne pense à l’identifiant créé pour celui-ci. Il reste simplement actif, non surveillé, parfois pendant des années. Un attaquant qui compromet cet ancien compte peut entrer dans votre réseau en semblant être un partenaire légitime, même ancien, ce qui le rend beaucoup plus difficile à repérer.

- **Les comptes oubliés sont un problème massif.** Un rapport 2025 a constaté que **88 % des organisations disposent de ces anciens comptes « utilisateurs fantômes »** dans leurs systèmes, prêts à être exploités.[42]

4. Intégrer la sécurité dans vos contrats.

Les discussions que vous avez avec vos fournisseurs au sujet de la sécurité sont importantes, mais vous devez mettre ces engagements par écrit. La meilleure façon de le faire consiste à ajouter une clause de sécurité simple ou une annexe d’une page à vos contrats avec vos fournisseurs à haut risque.

C’est important, car cela transforme la sécurité en obligation formelle et juridique. Cela fixe des attentes claires et écrites sur la manière dont vos données seront protégées et sur ce qui se passera si elles ne le sont pas.

Votre annexe de sécurité n'a pas besoin d'être un document juridique de 50 pages. Elle doit simplement couvrir quelques points de bon sens. Elle devrait obliger le fournisseur à maintenir des pratiques de sécurité raisonnables, comme celles évoquées dans ce guide : utiliser la MFA pour ses collaborateurs, maintenir ses systèmes à jour et chiffrer vos données.

Mais la partie la plus importante de cette clause contractuelle est l'**obligation de notification en cas de violation**. Votre contrat doit indiquer que si le fournisseur subit une violation de données qui affecte vos données, il doit vous en informer dans un délai court et précis, par exemple 24 ou 48 heures.

Plus vous apprenez tard qu'une violation a touché l'entreprise d'un partenaire, plus un attaquant peut causer de dégâts à votre entreprise. Une notification rapide vous donne la possibilité de réagir : couper ses accès, changer les mots de passe et vous protéger avant que le problème ne se propage.

- **Le délai de maîtrise d'une violation est critique.** Les données montrent clairement que les violations identifiées et contenues en moins de 200 jours coûtent en moyenne **1,39 million de dollars de moins** que celles qui prennent plus longtemps à détecter. Une obligation contractuelle de notification rapide peut vous faire économiser énormément d'argent.
- **Les violations impliquant des identifiants volés sont les plus longues à détecter.** Le délai moyen pour identifier et contenir une violation qui commence par un mot de passe volé est de **292 jours**. Si ce mot de passe volé appartient à votre fournisseur, vous pourriez ne rien savoir pendant des mois, sauf s'il est légalement obligé de vous en informer.[43]

ERREURS COURANTES À ÉVITER

Bien faire les choses importantes, c'est déjà la moitié du travail. L'autre moitié consiste à éviter quelques erreurs courantes qui peuvent annuler tous vos efforts.

Supposer qu'un fournisseur est sécurisé parce qu'il s'agit d'une marque connue.

Il est facile de supposer qu'une grande entreprise connue dispose d'une sécurité parfaite. Mais c'est une hypothèse dangereuse. Les grandes entreprises subissent elles aussi régulièrement des violations. En 2023, une seule vulnérabilité dans un outil populaire de transfert de fichiers appelé MOVEit a entraîné des violations chez des milliers d'organisations, y compris de nombreuses marques très connues.

En 2025, nous avons déjà vu des violations majeures impliquant de très grandes entreprises comme PowerSchool et Oracle Health, où un seul problème chez le fournisseur a affecté des millions de personnes. Lorsque vous connectez votre entreprise à un fournisseur, vous héritez de ses risques de sécurité, quelle que soit sa taille.

Vous devez effectuer vos propres vérifications de base et poser vos propres questions.

Souscrire à de nouveaux services logiciels sans revue de sécurité.

C'est souvent ce que l'on appelle le « shadow IT ». Un collaborateur doit résoudre un problème, il fait donc une recherche rapide sur Google, trouve un nouvel outil logiciel et s'y inscrit avec la carte de crédit de l'entreprise. Il a résolu son problème, mais il vient aussi de créer un nouveau risque de sécurité.

Vous avez maintenant des données sensibles de l'entreprise — peut-être une liste clients ou des informations financières — stockées dans un service que vous ne connaissez pas, que vous ne gérez pas et dont vous n'avez pas vérifié la sécurité. Vous ne pouvez pas protéger des données dont vous ignorez l'existence.

QUE DEMANDER À VOTRE PRESTATAIRE IT

Ces trois questions vous diront presque tout ce que vous devez savoir sur la qualité de gestion de votre risque fournisseurs.

- **« Pouvez-vous me fournir la liste de tous les comptes non-employés ayant accès à notre réseau ? Passons en revue qui en est responsable et quand leur accès doit expirer. »** Pour chaque compte de cette liste, il devrait y avoir le nom d'un collaborateur actuel qui en est responsable — le « propriétaire » — ainsi qu'une date à laquelle l'accès de ce compte sera automatiquement désactivé.
- **« Quel est notre processus pour revoir la sécurité d'un nouvel outil logiciel avant qu'un département commence à l'utiliser ? »** Il devrait s'agir d'un processus simple et rapide : si une équipe souhaite utiliser un nouvel outil, elle remplit un court formulaire, puis votre prestataire IT effectue une vérification rapide d'environ 15 minutes pour s'assurer que l'outil est raisonnablement sécurisé avant que des données de l'entreprise y soient déposées.
- **« Imaginons qu'un de nos fournisseurs à haut risque subisse une violation de sécurité. Pouvez-vous me décrire les étapes exactes que nous suivrions pour désactiver immédiatement son accès à nos systèmes ? »** C'est la question « et si ? » par excellence. Elle teste leur niveau de préparation face au pire scénario. Ils devraient disposer d'un plan documenté de coupure d'urgence, décrivant les étapes précises à suivre pour verrouiller immédiatement l'accès de ce fournisseur à vos systèmes et contenir les dégâts.

PARTIE III

La dernière couche de protection

Réponse aux incidents & continuité d'activité

Au risque de paraître pessimiste, il faut rappeler une évidence : une cyberattaque peut déstabiliser votre entreprise, entraîner une perte de chiffre d'affaires, nuire à votre réputation et créer des problèmes juridiques.

Ce n'est évidemment pas ce que vous souhaitez. Malheureusement, cela arrive parfois. Et, plus regrettable encore, beaucoup de petites entreprises ne disposent d'aucun plan clair indiquant quoi faire lorsqu'une attaque survient, ce qui les rend particulièrement vulnérables.

La bonne nouvelle — ou du moins la nouvelle rassurante — est que ce chapitre vous montre comment créer un plan simple et actionnable pour protéger votre entreprise et la maintenir en activité, même en pleine crise.

Votre plan doit comporter deux volets essentiels que l'on confond souvent, alors qu'ils répondent à des objectifs différents.

Le premier est votre plan de **réponse aux incidents**. C'est votre stratégie de « lutte contre l'incendie ».

Il se concentre sur le problème technique : stopper l'attaque, comprendre comment elle s'est produite et réparer les dégâts. L'objectif est de contenir le problème et de ramener vos systèmes dans un état sûr.

Le deuxième est votre plan de **continuité d'activité**. Celui-ci se concentre sur vos opérations métier.

Il explique comment vous continuerez à prendre des commandes, servir vos clients et payer les salaires pendant que le problème technique est en cours de résolution. Par exemple, si votre serveur principal est hors service, comment continuerez-vous à expédier vos produits ? Si votre système comptable est bloqué, comment enverrez-vous vos factures ? Ce plan permet à votre entreprise de continuer à fonctionner et à générer du chiffre d'affaires, même lorsque votre technologie ne fonctionne plus.

Un « incident » désigne tout événement qui menace votre capacité à fonctionner ou à protéger vos données. Il peut s'agir d'une attaque par rançongiciel, d'une panne serveur, d'un logiciel critique qui ne répond plus, d'un ordinateur portable volé contenant des données sensibles, ou même d'une coupure de courant. Si cela touche votre argent, vos données ou vos clients, considérez-le comme un incident et déclenchez votre plan.

Étape 1 : que faire avant que quoi que ce soit n'arrive — préparation

Votre préparation détermine en grande partie la manière dont vous gérerez un incident. Un bon plan est un guide court, simple, que vous pouvez utiliser rapidement lorsque vous en avez besoin.

Imprimez-le et conservez des copies dans des endroits sûrs et accessibles : dans votre bureau, à la maison, voire dans votre voiture. Ainsi, vous pourrez y accéder même si vos locaux sont inaccessibles ou si votre réseau informatique est hors service.

A. Désignez vos contacts

Votre plan doit contenir une liste simple de noms et de numéros de téléphone. Personne ne devrait devoir deviner qui appeler lorsque quelque chose tourne mal. Cette liste doit figurer en première page du plan. Elle

doit identifier les personnes qui formeront votre petite équipe de réponse aux incidents. Trois rôles principaux suffisent, et une même personne peut en assumer plusieurs.

- **Le responsable :** cette personne pilote la réponse globale. Elle prend les grandes décisions business, par exemple arrêter un système ou communiquer avec les clients. Il s'agit généralement de vous, du propriétaire de l'entreprise ou d'un autre membre de la direction.
- **Le contact technique :** c'est la première personne que chacun dans l'entreprise appelle s'il remarque quelque chose d'étrange. Elle lance l'investigation technique. Il peut s'agir de votre responsable IT interne ou de votre contact principal chez votre prestataire IT/MSP.
- **Le contact business/communication :** cette personne gère la communication avec les collaborateurs et les clients, et trouve des moyens de maintenir l'activité. Elle prend en charge le volet continuité d'activité.

Pour chaque personne, indiquez son nom, son rôle et son numéro de téléphone mobile personnel. Ne vous contentez pas d'une extension interne. En pleine crise, votre système téléphonique peut être indisponible ; vous devez donc disposer d'un moyen direct de la joindre.

Votre liste de contacts doit également inclure les interlocuteurs externes clés.

- **Votre cyber assureur :** si vous avez une police de cyber assurance, cela doit être votre tout premier appel. Vraiment. Faites-le immédiatement. La plupart des polices donnent accès à une hotline 24/7 avec une équipe d'experts — spécialistes forensiques, juristes et gestionnaires de crise — qui vous guideront dans le processus. Les appeler immédiatement est souvent une condition pour que votre demande d'indemnisation soit valable.
- **Les autorités compétentes :** vous devriez signaler l'incident aux autorités locales compétentes. Selon votre situation, vous devrez peut-être aussi le signaler aux autorités nationales ou régionales en matière de cybercriminalité. C'est important pour l'enquête et pour respecter d'éventuelles obligations légales.
- **Votre avocat :** ajoutez à cette liste les coordonnées du conseil juridique de votre entreprise. Vous aurez besoin de son avis sur vos responsabilités légales et réglementaires, surtout si des données clients sont concernées.

B. Identifier vos opérations critiques

C'est la partie « continuité d'activité » de votre préparation. Réunissez votre équipe et listez les activités de votre entreprise qui doivent absolument continuer à fonctionner.

Posez-vous des questions comme :

- Si notre serveur principal tombe en panne, comment continuons-nous à expédier nos produits ?
- Si notre système comptable est bloqué, comment envoyons-nous les factures et préparons-nous les salaires ?
- Si notre logiciel de gestion de la relation client (CRM) est indisponible, comment notre équipe commerciale suit-elle les prospects et les commandes ?

Pour chaque opération critique, définissez une solution de repli simple et manuelle. Si le système d'expédition est hors service, pouvez-vous passer à des bons de travail papier pendant un jour ou deux ?

Si le système comptable est indisponible, avez-vous un moyen de créer des factures simples à partir d'un modèle ?

Prévoir ces plans de secours évite que votre entreprise s'arrête complètement pendant que le problème technique est résolu. Cette liste indique aussi à votre équipe technique ce qu'elle doit rétablir en priorité.

C. Créer la règle « Stoppez et appelez » pour tout le personnel

C'est la règle la plus importante à enseigner à tout le monde dans votre entreprise. Si vous voyez quelque chose d'étrange sur votre ordinateur, arrêtez ce que vous faites et appelez immédiatement le contact technique figurant sur votre liste.

N'essayez pas de régler le problème vous-même. Ne terminez pas cet e-mail. Ne partez pas du principe qu'il s'agit simplement d'un bug. Arrêtez-vous et appelez.

C'est essentiel, car dans une cyberattaque moderne, chaque minute compte. Les attaquants utilisent des outils automatisés capables de se propager dans un réseau en quelques minutes.

Un rapport récent de Palo Alto Networks a constaté que, dans près d'un cas sur cinq, les attaquants volaient déjà des données durant la première heure suivant leur entrée dans un réseau.

Un collaborateur qui remarque quelque chose d'anormal et le signale immédiatement est souvent votre meilleure chance de contenir le problème avant qu'il ne devienne une crise à l'échelle de l'entreprise. À l'inverse, un collaborateur qui essaie de « terminer juste une dernière chose » peut faire la différence entre un problème limité à un ordinateur portable et une attaque par rançongiciel qui bloque toute l'activité.

D. Ne pas compter sur les « héros »

Lorsque vous rédigez ce plan, ne le faites pas dépendre d'une seule personne.

Il est facile de se dire : « On appellera simplement Bob », parce que Bob est votre génie IT et qu'il sait tout. Mais cela crée un point de défaillance unique.

Que se passe-t-il si l'incident survient à 2 h du matin et que le téléphone de Bob est éteint ? Ou s'il est en vacances ?

Votre plan doit être une checklist simple que n'importe quel responsable de l'entreprise peut prendre et suivre durant la première heure. Il doit être suffisamment clair pour permettre de prendre de bonnes décisions de base, même sous pression.

C'est d'autant plus important dans un contexte de pénurie généralisée de compétences en cybersécurité. Les données montrent que les violations dans les entreprises fortement touchées par ce manque de compétences coûtent des millions de plus que dans les autres.

Vous ne pouvez pas faire dépendre toute votre réponse de la disponibilité et de l'expertise d'une seule personne. L'objectif est de créer un processus ordonné et répétable que chacun peut suivre, plutôt que de compter sur une personne précise pour sauver la situation.

Étape 2 : que faire pendant un incident — action

Un incident vient d'être signalé. Quelqu'un dans votre équipe a appliqué la règle « Stoppez et appelez ».

C'est ici que votre préparation porte ses fruits. L'objectif est maintenant de passer de la réaction à l'action, en suivant le guide simple que vous avez déjà créé.

A. Contenir le problème

Votre première mission est d'empêcher le problème de s'aggraver. Pensez-y comme à un incendie : il faut d'abord l'éteindre avant de pouvoir reconstruire. Dans un incident cyber, cela s'appelle le confinement, et la rapidité est essentielle.

La première priorité consiste à isoler les ordinateurs affectés, sans les éteindre. Si l'ordinateur portable d'un collaborateur se comporte de manière étrange, votre contact technique doit immédiatement le retirer du réseau. Débranchez le câble réseau.

Désactivez le Wi-Fi. Mais laissez l'appareil allumé.

Cela empêche le problème de se propager depuis cet ordinateur vers votre serveur ou les autres ordinateurs du bureau.

Ensuite, changez tous les mots de passe susceptibles d'avoir été compromis. Si l'incident a commencé sur l'ordinateur d'un collaborateur, partez du principe que tous les mots de passe qu'il a utilisés ou enregistrés sur cette machine sont désormais entre les mains de l'attaquant.

Son mot de passe réseau principal, son mot de passe de messagerie et tous ses autres comptes importants doivent être changés immédiatement.

Enfin, stoppez tous les processus automatisés qui pourraient aggraver le problème.

Par exemple, si vous avez un système qui synchronise automatiquement des fichiers entre votre serveur et un service cloud, il peut être nécessaire de le mettre en pause. Sinon, il pourrait synchroniser des fichiers chiffrés par un rançongiciel vers votre stockage cloud, en écrasant vos bonnes copies.

Un autre point critique concernant le confinement : **vous DEVEZ préserver les preuves**.

Le premier réflexe en situation de crise est souvent de tout éteindre et de commencer à nettoyer. Vous devez résister à cette envie. Les ordinateurs affectés sont désormais une scène d'incident, et vous devez les traiter comme telle.

N'éteignez rien, sauf si votre expert technique vous le demande. Beaucoup de preuves importantes se trouvent dans la mémoire active de l'ordinateur et disparaissent dès que vous coupez l'alimentation.

Tenez un journal simple de chaque action effectuée, avec l'heure et le nom de la personne qui l'a réalisée. Cela sera extrêmement important pour l'enquête, ainsi que pour toute démarche ultérieure auprès de l'assurance ou sur le plan juridique.

- La rapidité est déterminante. Les données le montrent clairement. Un rapport 2025 de Palo Alto Networks a constaté que, dans près d'un cas sur cinq, les attaquants volaient déjà des données durant la première heure suivant leur entrée dans un réseau. Votre capacité à contenir rapidement le problème empêche un petit incident de devenir une violation majeure de données.

B. Maintenir l'activité

Pendant que votre équipe technique lutte contre l'incendie, vous devez maintenir l'activité de l'entreprise.

Imaginez une entreprise industrielle touchée par un rançongiciel un vendredi matin. Tous ses fichiers de conception et ses ordres de travail sont chiffrés. L'activité est bloquée. Mais comme elle avait un plan simple et déjà testé, l'équipe savait quoi faire.

Le responsable d'atelier a immédiatement demandé à l'équipe opérationnelle de passer au système de secours : des ordres de travail papier. Les lignes de production ont continué à tourner, plus lentement, mais elles ont continué. Le problème restait sérieux, mais il ne s'est pas transformé en catastrophe totale. L'entreprise pouvait encore servir ses clients les plus importants, car elle disposait d'une solution manuelle simple prête à l'emploi.

Voilà à quoi ressemble un plan de continuité d'activité dans la réalité.

Quelle est votre version des ordres de travail papier ? Comment continuez-vous à prendre des commandes si votre système principal est indisponible ? Comment envoyez-vous les factures ? Avoir ces réponses prêtes permet de continuer à générer du chiffre d'affaires pendant une crise.

C. Maîtriser la communication

Le silence est dangereux pendant une cyberattaque. Il crée des rumeurs, de la peur et de la panique. Si vous ne donnez pas d'informations, les collaborateurs et les clients feront leurs propres suppositions — souvent les pires.

Vous devez devenir la source unique et fiable d'information.

Vous n'avez pas besoin d'avoir toutes les réponses, surtout dans les premières heures. Mais vous devez communiquer ce que vous savez, et le faire régulièrement.

Communiquez trois choses simples à votre personnel et à vos clients clés :

- Ce que vous savez à ce stade, par exemple : « Nous avons une interruption système qui affecte notre capacité à traiter les commandes. »
- Ce que vous faites immédiatement, par exemple : « Notre équipe technique identifie le problème, et notre équipe opérationnelle bascule sur notre processus manuel de prise de commandes. »
- Quand vous donnerez la prochaine mise à jour, par exemple : « Nous vous tiendrons informés dans une heure, ou plus tôt si nous avons des informations importantes. »

Cela montre que vous gardez le contrôle, même si le problème n'est pas encore résolu.

Pour le faire efficacement, choisissez un canal de communication qui ne dépend pas des systèmes de votre entreprise.

Il peut s'agir d'un groupe de messages privé pour votre équipe de direction, ou d'une liste d'e-mails personnels pour tous les collaborateurs. Votre messagerie ou votre outil de chat d'entreprise peut être indisponible ; vous avez donc besoin d'un moyen fiable pour joindre tout le monde.

Étape 3 : que faire une fois l'incident terminé — revue

Une fois l'incendie éteint, les systèmes restaurés et l'activité revenue à la normale, il est tentant de pousser un soupir de soulagement et de passer à autre chose. Mais c'est l'une des parties les plus importantes de tout le processus.

Vous devez prendre le temps d'apprendre de ce qui s'est passé.

Ne vous précipitez toutefois pas pour chercher un coupable. Vous avez besoin d'une revue « sans blâme », destinée à rendre l'entreprise plus sûre, pas à punir les erreurs. Réunissez simplement votre petite équipe de réponse aux incidents pour une courte séance et posez deux questions simples :

- **Quelle était la cause racine du problème ?** Allez au-delà de la réponse superficielle. Un collaborateur a-t-il cliqué sur un lien de phishing ? Un attaquant est-il entré par un serveur non corrigé ? Quelqu'un a-t-il utilisé un mot de passe faible et volé sur un accès à distance sans authentification multifacteur (MFA) ? Vous devez identifier la véritable porte restée ouverte afin de pouvoir la verrouiller correctement.
- **Quelle ou quelles deux choses pouvons-nous changer pour éviter que cela ne se reproduise ?** Concentrez-vous sur une ou deux actions qui auraient fait la plus grande différence. Si le problème venait d'un e-mail de phishing, la solution peut être un meilleur outil de sécurité e-mail. Si le problème venait d'un serveur non corrigé, la solution peut être un calendrier de gestion des correctifs plus régulier. L'enquête britannique Cyber Security Breaches Survey 2025 a constaté qu'après un incident, le changement le plus fréquent était d'ajouter de la formation ou de la communication auprès du personnel. Quelle que soit l'action retenue, identifiez-la, attribuez-la à une personne avec une échéance, puis vérifiez qu'elle est bien réalisée.

Vous devez vous entraîner avec ce plan

Un plan qui reste simplement dans un classeur ne sert à rien. La seule façon de savoir s'il fonctionne est de le tester.

La meilleure façon de s'entraîner consiste à organiser un exercice simple d'une heure, appelé « exercice sur table ». Il s'agit d'une séance où vous et votre petite équipe de réponse aux incidents parcourez ensemble une crise fictive. C'est l'équivalent d'un exercice incendie, mais pour une cyberattaque.

Planifiez une séance d'une heure. Réunissez le responsable, le contact technique et le contact business dans une salle. Présentez-leur ensuite un scénario simple et réaliste.

« Nous sommes mardi, il est 9 h. Un collaborateur appelle et dit qu'un message étrange s'affiche sur son écran, demandant un paiement en bitcoins, et qu'aucun de ses fichiers ne s'ouvre. Cela ressemble à une attaque par rançongiciel. Que faisons-nous maintenant ? »

Ensuite, déroulez le scénario étape par étape. Qui appelle qui en premier ? Quelle est la première action de la personne technique ? Comment informons-nous le reste du personnel ? Quel est notre plan pour maintenir l'activité si le serveur principal est hors service ?

En discuter calmement vous aide à repérer les failles dans votre plan. Vous découvrirez peut-être que le numéro de contact de votre prestataire IT est incorrect, que la personne qui doit prendre une décision clé est en vacances sans remplaçant, ou que votre solution de secours avec des ordres de travail papier ne fonctionne pas parce que les modèles se trouvent sur le serveur chiffré.

- **Tester votre plan permet d'économiser beaucoup d'argent.** Un rapport IBM 2025 a constaté que les entreprises qui testent régulièrement leurs plans de réponse aux incidents économisent en moyenne **1,49 million de dollars par violation** par rapport à celles qui ne le font pas.

1,49 M$

économisés par violation par les entreprises qui testent leur plan de réponse aux incidents

- **Le manque de planification coûte cher.** La même étude a constaté que les entreprises sans plan formel et testé de réponse aux incidents payaient **58 % de plus par violation** que celles qui étaient préparées.
- **La plupart des entreprises ne le font pas.** Malgré le bénéfice financier évident, beaucoup d'entreprises sautent cette étape. Un rapport a constaté que **seules 30 % des organisations testent régulièrement leurs plans de réponse aux incidents**. En réalisant ce simple exercice d'une heure quelques fois par an, vous serez bien mieux préparé que la majorité de vos pairs.

Conformité & gouvernance pour PME

Nous entrons maintenant dans un sujet un peu moins glamour. La conformité est souvent perçue comme ennuyeuse, et ce n'est probablement pas le chapitre que vous attendiez avec le plus d'impatience.

Elle peut sembler lourde, complexe et remplie de jargon. C'est précisément pour cette raison que ce chapitre simplifie la conformité et la gouvernance, afin d'en faire un ensemble d'habitudes concrètes, vérifiables et faciles à gérer.

Commençons par clarifier ce que ces termes signifient. Même s'ils sont souvent utilisés comme s'ils étaient interchangeables, ils ont des rôles différents :

- **La sécurité** correspond aux mesures concrètes que vous mettez en place pour protéger votre entreprise. Cela inclut la protection moderne des terminaux, les tests de restauration des sauvegardes, la gestion des accès et la sensibilisation de votre équipe au phishing. C'est l'équivalent des serrures, des alarmes et des caméras dans vos locaux.
- **La conformité** consiste à démontrer que votre entreprise respecte des règles précises. Ces règles peuvent venir de la loi — par exemple la nLPD ou le RGPD —, de votre secteur d'activité, d'un cyberassureur ou d'un client important qui veut vérifier que vous êtes un partenaire fiable. C'est l'équivalent de pouvoir présenter les preuves d'entretien de votre système anti-incendie lorsqu'un inspecteur les demande.
- **La gouvernance** désigne la manière dont les responsabilités sont attribuées, dont les décisions sont prises et dont les contrôles sont suivis dans le temps. Elle garantit qu'une personne est responsable du programme de sécurité et que les progrès sont revus régulièrement.

Vous avez besoin des trois.

Une bonne sécurité sans preuves rend plus difficile l'obtention de grands clients ou d'une cyberassurance solide. À l'inverse, une conformité uniquement « sur papier », sans contrôles réels derrière, reste fragile.

Les pages suivantes vous aideront à mettre en place un système simple et pratique, qui couvre ces trois dimensions sans créer une montagne de documents inutiles.

Un plan simple et pratique

Vous n'avez pas besoin d'une équipe dédiée à la conformité pour y parvenir. Il vous faut surtout un plan simple, fondé sur quelques habitudes régulières : choisir un cadre, désigner un responsable, vérifier les contrôles et conserver les preuves.

A. Utiliser votre cadre comme guide

Vous n'avez pas besoin — et vous ne devriez pas — repartir de zéro.

Souvenez-vous du chapitre consacré aux cadres de sécurité. Ce cadre est votre guide.

Il liste les étapes essentielles pour protéger votre entreprise et les éléments que vous devrez, à terme, être capable de prouver.

Que vous utilisiez le standard minimal TIC du NCSC, les contrôles CIS, le cadre NIST ou ISO 27001, l'idée reste la même : choisissez un cadre de référence et suivez-le de manière cohérente.

Un seul bon cadre suffit pour structurer votre programme et garder le cap sur ce qui compte vraiment.

B. Désigner un responsable

Le mot « gouvernance » peut sembler très formel. Pour une PME, il signifie surtout qu'une personne de votre équipe est clairement responsable du programme de sécurité. Cela ne doit pas forcément être un poste à plein temps ; dans la plupart des petites entreprises, il s'agit d'une responsabilité à temps partiel.

Mais quelqu'un doit en être propriétaire. Quelqu'un doit s'assurer que les sauvegardes sont testées, que les mises à jour de sécurité sont installées, que les accès sont revus et que les preuves sont conservées. Si « tout le monde » est responsable, alors personne ne l'est vraiment. Le simple fait de désigner un responsable vous place déjà devant de nombreuses entreprises où la responsabilité cyber au niveau de la direction reste floue.

C. Fixer un rythme régulier

Une fois le responsable désigné, fixez un rythme régulier pour suivre les sujets de sécurité et de conformité. Une courte séance mensuelle de 30 minutes avec le responsable sécurité, éventuellement accompagné de la personne en charge des finances ou des opérations, suffit.

Pendant cette séance, posez trois questions simples :

1. **« Qu'est-ce qui a changé dans l'entreprise ce mois-ci ? »** Avez-vous engagé de nouvelles personnes ? Démarré un nouveau logiciel ? Signé un nouveau client ? Tout changement business peut créer un nouveau risque de sécurité ; il faut donc en parler.
2. **« Avons-nous eu des incidents de sécurité ou des quasi-incidents ? »** Quelqu'un a-t-il signalé un e-mail de phishing convaincant ? Un outil de sécurité a-t-il envoyé une alerte ? Discuter des quasi-incidents permet d'identifier et de corriger de petits problèmes avant qu'ils ne deviennent graves.
3. **« Quels contrôles vérifions-nous ce mois-ci ? »** Vous ne pouvez pas tout vérifier chaque mois. Choisissez quelques contrôles prioritaires. Par exemple, ce mois-ci, vérifiez le rapport montrant que tous les ordinateurs portables sont chiffrés. Le mois prochain, contrôlez le journal du dernier test de restauration de sauvegarde.

L'habitude de « conserver les preuves » — votre documentation

La documentation fait souvent soupirer les dirigeants d'entreprise, mais elle n'a pas besoin de devenir un projet énorme et chronophage.

Vous devez simplement prendre l'habitude de conserver les preuves au fur et à mesure. C'est ce que vous présenterez lorsqu'un grand client, votre cyberassureur ou un auditeur vous demandera de démontrer que vos contrôles de sécurité fonctionnent.

Vous n'avez besoin que de trois éléments :

- **Politiques :** ce sont de courts documents qui indiquent « ce que nous faisons ». Par exemple, une politique d'une page peut dire : « Tous les collaborateurs doivent utiliser l'authentification multifacteur sur leur messagerie, et tous les ordinateurs portables de l'entreprise doivent être chiffrés. » C'est une déclaration claire de vos règles.
- **Procédures :** ce sont des instructions étape par étape qui expliquent « comment nous le faisons ». Par exemple, un guide d'une page avec des captures d'écran peut montrer à un nouveau collaborateur comment configurer la MFA sur son téléphone.
- **Preuves :** ce sont les éléments qui démontrent que vos contrôles fonctionnent réellement. Il peut s'agir de captures d'écran, de rapports, de journaux ou de notes de réunion. Par exemple : une capture du tableau de bord Microsoft 365 montrant que la MFA est activée pour tous les utilisateurs, un rapport de sauvegarde confirmant un test de restauration réussi, ou les notes de votre revue mensuelle de sécurité.

Lorsque vous réalisez une vérification de contrôle, comme un test de restauration ou une revue des accès, enregistrez la preuve dans un dossier clairement nommé avec l'année et le mois, par exemple « 2025-10 Preuves ».

Puis, dans les notes de votre revue mensuelle, ajoutez une ligne simple : « Test de restauration trimestriel effectué, rapport enregistré dans le dossier des preuves. » Cela prend deux minutes de plus, mais lorsqu'un auditeur vous demandera dans un an de prouver que vous avez réalisé un test de restauration, vous disposerez d'une trace claire, datée et prête à présenter.

Gérer les audits & questionnaires

Un audit consiste simplement à ce que quelqu'un vérifie vos contrôles et vos preuves. Qu'il s'agisse de votre cyber assureur, d'un client potentiel ou d'un régulateur, on vous demande de démontrer que vous prenez des mesures de base, raisonnables et concrètes pour protéger votre entreprise.

Si vous avez pris l'habitude de conserver vos preuves, ce processus devient beaucoup plus simple. Lorsqu'un auditeur demande : « Avez-vous une politique pour l'authentification multifacteur ? », vous fournissez la politique d'une page que vous avez déjà.

Lorsqu'il demande : « Pouvez-vous prouver que tous vos collaborateurs l'utilisent ? », vous ouvrez votre dossier de preuves, récupérez la capture d'écran du contrôle du mois précédent et la transmettez.

Cela montre que vous êtes professionnel, organisé et que votre programme de sécurité est réellement intégré à la gestion de votre entreprise.

La même logique s'applique aux longs questionnaires de sécurité envoyés par de grands clients. Votre cadre de référence devient votre base de réponse. Les questions posées correspondent presque toujours aux contrôles essentiels de ce cadre.

Vous pouvez créer un document simple avec des réponses standards aux questions fréquentes, à partir de vos politiques et de vos preuves. La première fois, cela peut prendre un peu de temps, mais les fois suivantes seront beaucoup plus rapides, car vous aurez déjà fait le travail et conservé les réponses.

UNE COURTE NOTE SUR LA PROTECTION DES DONNÉES

Si votre entreprise traite des données personnelles — ce qui est le cas de presque toutes les entreprises, ne serait-ce que pour les informations des collaborateurs — vous êtes responsable de leur protection. Ce sujet prend de plus en plus d'importance, et les exigences deviennent plus strictes.

Vous n'avez pas besoin d'être juriste pour comprendre les principes de base :

- Soyez clair sur les raisons pour lesquelles vous collectez des données.
- Obtenez le consentement lorsque cela est nécessaire.
- Ne conservez que les données dont vous avez réellement besoin pour votre activité.
- Supprimez les données de manière sécurisée lorsque vous n'avez plus de raison valable de les conserver.

Une déclaration de confidentialité claire sur votre site web expliquant ces points constitue un bon début. Toutefois, c'est un domaine dans lequel il vaut la peine de consulter un avocat. Les règles précises peuvent varier fortement selon les pays où vous exercez votre activité et où se trouvent vos clients.

Par exemple, si vous avez des clients européens, le RGPD peut s'appliquer. En Suisse, vous devez également tenir compte de la nLPD.

Les conséquences d'une non-conformité peuvent être importantes. Le coût moyen d'une violation de données est déjà élevé, mais pour les entreprises présentant un niveau élevé de non-conformité, ce coût est en moyenne 12,6 % plus élevé.

Une courte discussion avec un juriste compétent peut éviter de gros problèmes plus tard.

Transformer la conformité en routine maîtrisable

Pour relier tout cela et le maintenir mois après mois, utilisez un outil simple : un « registre des contrôles ».

Il s'agit d'un tableur qui liste vos principaux contrôles de sécurité et de conformité. C'est la liste de suivi centrale de votre programme, avec des colonnes pour :

- Quel est le contrôle ? Par exemple : « Test de restauration de sauvegarde ».
- Qui en est responsable ? Par exemple : « Notre prestataire IT ».
- À quelle fréquence doit-il être vérifié ? Par exemple : « Trimestriel ».
- Où se trouve la preuve ? Par exemple : « Dossier Preuves ».

Utilisez ce registre lors de votre revue mensuelle de 30 minutes. Le responsable sécurité l'ouvre, identifie les contrôles à vérifier ce mois-ci et demande la preuve au propriétaire concerné.

N'attendez pas qu'un client, un cyber assureur ou un régulateur vous demande des preuves pour commencer à les collecter. C'est la plus grande erreur à éviter. Essayer de reconstituer après coup une année entière de preuves est chronophage, stressant et donne une impression peu professionnelle.

Vous pourriez même ne pas retrouver la preuve dont vous avez besoin. Il est beaucoup plus simple de consacrer quelques minutes chaque mois à enregistrer une capture d'écran, un rapport ou une note de revue.

Conclusion

Mon objectif avec ce guide était de vous donner une voie claire et réaliste pour protéger votre entreprise, sans vous transformer en expert en cybersécurité.

J'espère qu'il vous aura été utile et que vous comprenez maintenant mieux ce qu'est la cybersécurité — mais surtout quelles habitudes mettre en place pour protéger votre entreprise contre les menaces modernes.

Comme vous l'avez vu, la plupart des gains en sécurité ne viennent pas de l'achat des outils les plus chers ou les plus complexes. Ils viennent du fait de bien faire les fondamentaux, de manière répétée.

Si vous ne deviez retenir que quelques idées clés de ce guide, j'aimerais que ce soient celles-ci :

- **Contrôlez les accès.**

> *Vous devez garder le contrôle sur les personnes qui détiennent les clés de votre entreprise.*
>
> *Cela signifie utiliser l'authentification multifacteur partout, sans exception.*
>
> *C'est l'action la plus efficace que vous puissiez mettre en place — et vous pouvez commencer dès aujourd'hui.*
>
> *Cela signifie aussi disposer d'une liste de tous les appareils utilisés pour le travail, et vérifier qu'ils sont sécurisés.*
>
> *Enfin, cela signifie retirer les droits administrateur aux collaborateurs pour leur travail quotidien.*
>
> *Ce n'est pas de la science-fiction : c'est simple, concret et important.*

- **Sachez où se trouvent vos données.**

> *Vous ne pouvez pas protéger vos informations les plus importantes si vous ne savez pas où elles se trouvent.*
>
> *Définissez des emplacements autorisés précis pour vos données sensibles, par exemple un dossier serveur spécifique ou votre logiciel comptable.*
>
> *Et empêchez le partage public de fichiers par défaut.*
>
> *Une simple mauvaise configuration dans votre stockage cloud est l'un des moyens les plus fréquents par lesquels des entreprises exposent de grandes quantités de données.*
>
> *Et c'est précisément le genre de situation que vous voulez éviter.*
>
> *Ayez un plan lorsque les choses tournent mal.*
>
> *Je ne veux pas être pessimiste, mais quelque chose finira par mal tourner. Ce n'est pas une question de « si », mais de « quand ».*
>
> *Ce qui fera la différence entre un problème maîtrisable et une catastrophe, c'est l'existence d'un plan.*
>
> *Cela signifie tester la restauration de vos données depuis vos sauvegardes, afin de savoir avec certitude que cela fonctionne.*
>
> *Cela signifie organiser de courts exercices sur table d'une heure pour répéter votre plan de réponse aux incidents.*
>
> *Et cela signifie garder ce plan sur une page, avec les noms et numéros de téléphone des personnes à appeler tout en haut.*

> *Par exemple : cyber assureur, prestataire IT, avocat, autorités compétentes, etc.*

- **Séparez vos réseaux.**

> *Votre réseau ne devrait pas ressembler à une grande pièce ouverte. Vous devez y installer quelques murs simples.*
>
> *Au minimum, gardez vos invités sur un réseau Wi-Fi séparé de celui de votre entreprise.*
>
> *Placez aussi les appareils moins sécurisés — téléviseurs connectés, caméras de sécurité ou équipements similaires — dans une zone séparée.*
>
> *C'est ce qui empêche un problème sur l'ordinateur d'un visiteur de se propager à votre serveur principal.*

- **Gérez le risque fournisseurs.**

> *Un problème chez l'un de vos fournisseurs peut rapidement devenir votre problème.*
>
> *Classez vos fournisseurs par niveau de risque et concentrez votre attention sur ceux qui sont critiques pour votre activité.*
>
> *Pour ces fournisseurs à haut risque, exigez des comptes nominatifs, uniques et assortis d'une date d'expiration.*
>
> *Et lorsque c'est possible, ajoutez une annexe de sécurité simple à vos contrats.*
>
> *Elle doit les obliger à vous informer rapidement en cas d'incident de sécurité.*

- **Demandez des preuves, ne supposez pas.**

> *Vous ne pouvez pas simplement espérer que votre sécurité fonctionne. Vous devez vérifier.*
>
> *C'est l'habitude de conserver des preuves.*
>
> *Prenez l'habitude d'enregistrer chaque mois des rapports et captures d'écran datés comme preuves du bon fonctionnement de vos contrôles.*
>
> *C'est le rapport qui montre que tous vos ordinateurs portables sont chiffrés.*
>
> *C'est la capture qui montre que tous vos collaborateurs utilisent la MFA.*
>
> *Et cela signifie que vos politiques écrites doivent être courtes, simples et alignées avec ce que vous faites réellement.*

Dernier point, mais non des moindres : **la sécurité est une habitude.**

C'est le changement d'état d'esprit le plus important. La sécurité n'est pas un projet. Un projet a un début et une fin. La sécurité, elle, ne se « termine » jamais.

C'est une habitude, une routine, au même titre que tenir votre comptabilité, gérer votre stock ou fermer les bureaux le soir. C'est une partie normale et continue de la gestion d'une entreprise professionnelle.

Lorsque vous abordez la sécurité de cette manière, elle cesse d'être un sujet immense, inquiétant et paralysant. Elle devient une série de petites tâches maîtrisables : vérifier les sauvegardes, revoir les accès,

s’assurer que les logiciels sont à jour. Ces tâches peuvent — et devraient — être suivies avec l’appui de votre prestataire IT/MSP.

La vraie valeur de cette routine apparaît le jour où quelque chose tourne mal.

Parce que vous avez un plan et que vous l’avez testé, votre équipe peut répondre avec une séquence claire d’actions au lieu de paniquer.

Elle saura qui appeler, quoi faire en premier et comment maintenir l’activité. Cette préparation a un impact financier massif et mesurable. IBM a constaté que les entreprises qui testent régulièrement leurs plans de réponse aux incidents économisent en moyenne **1,49 million de dollars par violation** par rapport à celles qui ne le font pas. La même étude a également montré que les entreprises sans plan formel et testé de réponse aux incidents payaient **58 % de plus par violation** que celles qui étaient préparées.

Une dernière chose avant de partir

Si vous êtes arrivé jusqu’ici, bravo.

La plupart des dirigeants ne prennent jamais le temps de réfléchir sérieusement à la cybersécurité et aux étapes nécessaires pour la mettre en œuvre correctement. Vous avez investi ce temps, et vous disposez maintenant d’une vision claire des actions nécessaires pour protéger votre entreprise contre les menaces modernes.

Pour vous remercier d’avoir lu ce guide et de prendre votre sécurité au sérieux, je souhaite vous offrir un **bonus lecteur** personnel : **un appel de conseil gratuit de 30 minutes avec moi.**

Parfois, même après avoir lu un guide, une courte discussion suffit pour vérifier que vous démarrez dans la bonne direction. Cet appel est l’occasion de poser les questions qui vous semblent les plus importantes concernant votre sécurité.

Pendant notre échange, nous pouvons nous concentrer sur ce qui est le plus critique pour vous maintenant. Je peux vous aider à :

- **Prioriser** les une ou deux habitudes de sécurité à plus fort impact pour votre entreprise.
- Identifier la principale faiblesse de sécurité facile à corriger, celle qu’il faut traiter en priorité.
- **Obtenir des réponses claires** sur les sujets de ce guide qui resteraient encore flous.

Pour planifier votre appel, contactez-nous simplement :

Envoyez-nous un e-mail à : mail@awsmtech.ch

Ou appelez-nous au : +41 (0) 22 552 60 70

Merci pour votre lecture, et je vous souhaite plein succès dans la sécurisation de votre entreprise !

Bien à vous,

Andrea C. Nuti
Co-fondateur

Glossaire — décodeur de jargon

Bienvenue dans le décodeur de jargon de la cybersécurité.

Ce dernier chapitre vous aide à comprendre les termes les plus importants et les plus couramment utilisés dans le domaine. Il vous sera utile lorsque vous mettrez en pratique les recommandations de ce guide, ou lorsque vous échangerez avec vos prestataires IT, assureurs et fournisseurs.

Le décodeur de A à Z : 30 termes que tout dirigeant devrait connaître

1. **Authentification**
   Mécanisme qui permet de vérifier qu'une personne est bien celle qu'elle prétend être, par exemple au moyen d'un mot de passe, d'un code ou d'une validation sur téléphone.
2. **Botnet**
   Réseau d'ordinateurs ou d'appareils infectés, contrôlés à distance par un criminel pour lancer des attaques à grande échelle, comme envoyer du spam ou saturer un site web.
3. **Compromission d'e-mail professionnel (BEC)**
   Fraude par e-mail dans laquelle un criminel se fait passer pour une personne de confiance — dirigeant, fournisseur ou collègue — afin d'obtenir un paiement ou des informations sensibles.
4. **Cloud computing**
   Utilisation de serveurs, logiciels ou espaces de stockage fournis via Internet par un prestataire externe, plutôt que gérés directement dans vos propres locaux.
5. **Conformité**
   Capacité à démontrer que votre entreprise respecte les règles applicables en matière de sécurité, de protection des données ou d'exigences contractuelles.
6. **Cyber assurance**
   Assurance destinée à couvrir certains coûts liés à un incident cyber, comme l'assistance d'experts, la restauration des systèmes, les frais juridiques ou l'interruption d'activité.
7. **Attaque DDoS — déni de service distribué**
   Attaque qui rend un site web ou un service en ligne indisponible en l'inondant de trafic inutile provenant de nombreux appareils, jusqu'à empêcher les vrais utilisateurs d'y accéder.
8. **Chiffrement**
   Technique qui transforme des données lisibles en données illisibles pour toute personne ne disposant pas de la clé ou du mot de passe nécessaire.
9. **EDR — détection et réponse sur les terminaux**
   Outil de sécurité moderne qui surveille les ordinateurs et serveurs à la recherche de comportements suspects, puis aide à contenir rapidement une attaque.
10. **Pare-feu**
    Système de sécurité qui filtre le trafic entre votre réseau interne et Internet, afin d'autoriser les connexions légitimes et de bloquer les accès non souhaités.
11. **Réponse aux incidents**
    Ensemble des actions prévues pour détecter, contenir, analyser et résoudre un incident de sécurité ou informatique majeur.
12. **Adresse IP**
    Adresse numérique qui identifie un appareil sur Internet ou sur un réseau interne, un peu comme une adresse postale identifie un bâtiment.

13. **Malware — logiciel malveillant**
    Terme général désignant tout logiciel conçu pour voler des informations, perturber un système ou aider un attaquant à prendre le contrôle d'un appareil.

14. **Prestataire de services managés (MSP)**
    Entreprise IT qui gère de manière continue les systèmes, les utilisateurs, les appareils et souvent la cybersécurité de ses clients.

15. **Authentification multifacteur (MFA)**
    Méthode de connexion qui exige plusieurs preuves d'identité, par exemple un mot de passe et une validation sur téléphone, afin de bloquer l'usage d'un mot de passe volé.

16. **Segmentation réseau**
    Découpage du réseau informatique en zones séparées, par exemple réseau interne, Wi-Fi invité et appareils moins sécurisés, afin de limiter la propagation d'une attaque.

17. **Gestion des correctifs**
    Processus consistant à installer régulièrement les mises à jour de sécurité afin de corriger les failles connues avant qu'elles ne soient exploitées.

18. **Test d'intrusion**
    Exercice contrôlé durant lequel des spécialistes tentent de pénétrer dans vos systèmes, avec votre accord, afin d'identifier les faiblesses avant les criminels.

19. **Phishing**
    Message frauduleux — e-mail, SMS ou chat — conçu pour pousser une personne à cliquer sur un lien dangereux, ouvrir une pièce jointe ou révéler des informations sensibles.

20. **Rançongiciel**
    Logiciel malveillant qui chiffre vos fichiers ou bloque vos systèmes, puis exige une rançon pour tenter de les récupérer.

21. **Remote Desktop Protocol (RDP)**
    Fonction Windows permettant de contrôler un ordinateur à distance. Mal sécurisé ou exposé directement à Internet, il devient une porte d'entrée fréquente pour les attaquants.

22. **Risque**
    Combinaison entre la probabilité qu'un incident se produise et l'impact qu'il aurait sur votre entreprise.

23. **Serveur**
    Ordinateur ou système qui fournit des services à d'autres appareils, par exemple le stockage de fichiers, l'hébergement d'applications ou la gestion des connexions.

24. **Ingénierie sociale**
    Technique de manipulation qui vise à tromper une personne pour qu'elle révèle des informations, effectue un paiement ou réalise une action risquée.

25. **Acteur de la menace**
    Personne, groupe criminel ou organisation capable de mener une cyberattaque contre une entreprise, un système ou des données.

26. **Authentification à deux facteurs (2FA)**
    Forme d'authentification multifacteur qui utilise exactement deux preuves d'identité, par exemple un mot de passe et un code temporaire.

27. **VPN — réseau privé virtuel**
    Outil qui crée une connexion chiffrée entre un appareil et le réseau de l'entreprise, souvent utilisé pour accéder aux ressources internes à distance.

28. **Vulnérabilité**
    Faiblesse dans un logiciel, un appareil, une configuration ou un processus, qu'un attaquant pourrait exploiter pour causer un dommage.

29. **Exploit zero-day**
    Attaque qui exploite une vulnérabilité inconnue du fournisseur ou pas encore corrigée, ce qui laisse peu ou pas de temps pour se protéger.

30. **Zero Trust — confiance zéro**
    Modèle de sécurité fondé sur le principe « ne jamais faire confiance par défaut, toujours vérifier », avec une validation régulière des utilisateurs, appareils et accès.

Références

[1]: https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf

[2]: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

[3]: https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/ / https://www.verizon.com/business/resources/reports/dbir/

[4]: https://www.fbi.gov/news/press-releases/fbi-releases-annual-internet-crime-report/

[5]: Cost of a data breach 2025 \| IBM

[6]: https://www.verizon.com/business/resources/reports/dbir/

[7]: https://hoxhunt.com/guide/phishing-trends-report

[8]: https://gurucul.com/2024-insider-threat-report/

[9]: https://www.fortinet.com/resources/articles/credential-compromise-attacks

[10]: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index

[11]: https://deepstrike.io/blog/vulnerability-statistics-2025

[12]: https://deepstrike.io/blog/vulnerability-statistics-2025

[13]: https://securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/

[14]: https://securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/

[15]: https://www.fortinet.com/resources/cyberglossary/ransomware-statistics

[16]: https://ddos-guard.net/blog/ddos-trends-2025-mid-year

[17]: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1/ / https://ddos-guard.net/blog/ddos-trends-2025-mid-year

[18]: https://scoop.market.us/multi-factor-authentication-statistics/

[19]: https://spacelift.io/blog/password-statistics

[20]: https://spacelift.io/blog/password-statistics

[21]: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[22]: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[23]: https://nvd.nist.gov/general/nvd-dashboard

[24]: https://www.paloaltonetworks.com/blog/2025/02/incident-response-report-attacks-shift-disruption/

[25]: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

[26]: https://www.verizon.com/business/resources/reports/dbir/

[27]: https://www.verizon.com/business/resources/reports/dbir/

[28]: https://hoxhunt.com/guide/phishing-trends-report

[29]: https://www.verizon.com/business/resources/reports/dbir/

[30]: https://www.crowdstrike.com/en-us/resources/reports/threat-hunting-report/

[31]: http://varonis.com/blog/state-of-data-security-report

[32]: https://www.veeam.com/blog/announcing-rw24.html

[33]: https://www.sophos.com/en-us/content/state-of-ransomware

[34]: https://www.unitrends.com/resources/the-state-of-backup-and-recovery-report-2025/

[35]: https://www.unitrends.com/resources/the-state-of-backup-and-recovery-report-2025/

[36]: https://info.varonis.com/en/state-of-data-security-report-2025

[37]: https://www.verizon.com/business/resources/reports/dbir/

[38]: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[39]: https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report

[40]: https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf

[41]: https://securityscorecard.com/company/press/securityscorecard-2025-global-third-party-breach-report-reveals-surge-in-vendor-driven-attacks/

[42]: http://varonis.com/blog/state-of-data-security-report

[43]: https://www.ibm.com/reports/data-breach