Cyber-risques

Qu'est-ce qu'un cyber-risque ?

Le terme cyber-risque regroupe l'ensemble des risques et dangers liés à l'usage des technologies numériques susceptibles de compromettre la confidentialité, l'intégrité, l'authenticité ou la disponibilité des données et des outils de production.

Aucune entreprise n'est à l'abri, quelle que soit sa taille, la nature de son activité ou son secteur (commerce, services, santé, finance, industrie, etc.). Il suffit d'un incident pour mettre en péril toute l'activité d'une entreprise.

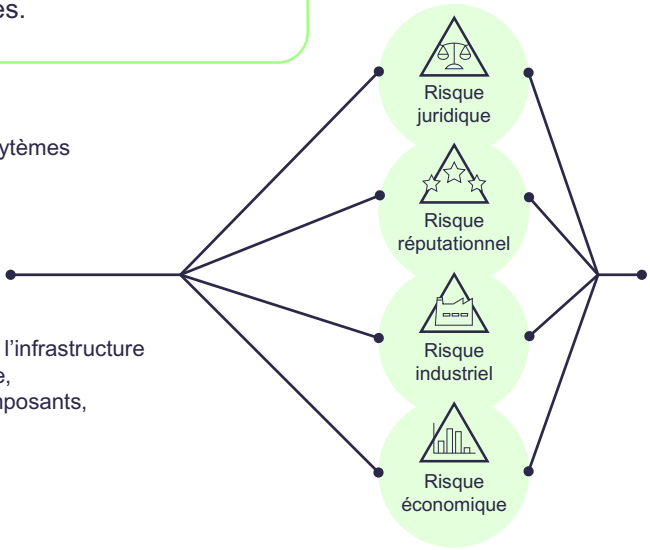
Soyez vigilant : prenez les bonnes décisions et appliquez les bonnes pratiques.

Dangers liés aux cyber-risques

En compromettant la sécurité de données, qu'elles soient sensibles ou non, les cyber-risques peuvent avoir de lourdes conséquences comme des pertes financières, l'interruption des activités commerciales, la perturbation de l'activité, des risques de sécurité, l'arrêt de la production ou des dommages à la réputation.

Risques internes
Négligence, mauvais usage des sytèmes informatiques ou des données, erreur humaine, malveillance, manque de formation, etc.

Risques externes
Attaque informatique, incident sur l'infrastructure tel que dégât des eaux et incendie, pénurie d'énergie, pénurie de composants, incendie chez un partenaire, évolution réglementaire, etc.



Prévention et réduction des risques
Plusieurs actions permettent de réduire les cyber-risques : mise en œuvre des politiques de sécurité, formation des employés, mise en place des procédures de secours et de récupérations.

« Dans le monde interconnecté dans lequel nous vivons, les menaces cybernétiques sont une réalité incontournable. Il est impératif de prendre toutes les mesures pour protéger au mieux son entreprise, ses collaboratrices et collaborateurs. »

Dimitri Konstantas, Professeur et Directeur du Information Science Institute de l'Université de Genève

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

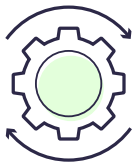
h e g
Haute école de gestion Genève

UNIVERSITÉ DE GENÈVE

En savoir +

Les indispensables

Protégez vos fichiers et vos appareils

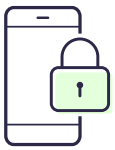


Gardez vos logiciels et systèmes à jour en appliquant les mises à jour automatiques de vos applications, navigateurs web, systèmes d'exploitation, appareils et équipements.

Verrouillez l'accès aux appareils (ordinateurs, tablettes, smartphones, etc.) avec un mot de passe fort généré par vous-même ou un service de gestion de mots de passe, et ne les laissez pas sans surveillance dans des lieux publics. Faites preuve de prudence lorsque vous utilisez des réseaux Wi-Fi publics.

Imposez l'authentification multifacteur pour accéder à votre réseau d'entreprise (SMS, e-mail, application d'authentification, etc.).

Sauvegardez vos fichiers importants hors-ligne, sur disque dur externe ou dans le cloud pour pouvoir y accéder même lors d'une perte, d'une panne ou du vol de votre équipement. Assurez-vous également de stocker vos dossiers papier de manière sécurisée.



Utilisez une clé de chiffrement pour protéger les informations sensibles et critiques qui se trouvent sur les appareils de votre entreprise, tels que les ordinateurs portables, tablettes, smartphones, disques durs amovibles et clés USB, ainsi que les solutions de stockage en cloud.

Ayez recours à des logiciels et/ou des systèmes de protection (antivirus, pare-feu, système de détection et de prévention d'intrusion (IDS/IPS) etc…).

La sécurité de votre entreprise est primordiale !
Faites-vous accompagner par des spécialistes.

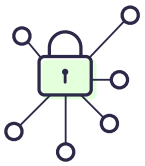
Les indispensables

Protégez votre réseau

Activez votre pare-feu (firewall) pour contrôler et filtrer le trafic réseau en autorisant ou en bloquant certains types de communications et contenus en fonction de règles prédéfinies.

Sécurisez votre routeur en changeant le nom et le mot de passe par défaut et en désactivant la gestion à distance. Pensez à changer régulièrement le mot de passe.

Assurez-vous que votre réseau sans fil offre un cryptage WPA2 ou WPA3 et qu'il est activé pour protéger les informations qui transitent sur votre réseau contre des personnes non autorisées.



Définissez des listes restrictives d'appareils autorisés à accéder au réseau de l'entreprise.

Renommez le nom par défaut de votre réseau Wi-Fi afin que celui-ci ne permette pas de vous identifier. Pour plus de discrétion, vous pouvez le masquer.

Faites de la sécurité une culture d'entreprise

Créez une culture de la sécurité en formant régulièrement vos équipes et en les informant des nouveaux risques et des nouvelles vulnérabilités.

Mettez en place un **Plan de continuité des activités (PCA)**. Ce plan doit décrire la manière de sauvegarder vos données et de maintenir votre entreprise en activité dans le cas d'un incident, d'une attaque ou d'un dégât. Mettez ce plan par écrit, communiquez-le à toutes les personnes concernées au sein de votre entreprise et testez-le régulièrement.

Établir une stratégie

Comment réduire les cyber-risques en entreprise ?

Quelle que soit leur taille, toutes les entreprises sont concernées par la mise en œuvre des **5 étapes** suivantes.

1 Identifier

- Faites une liste de tous les équipements, applications et services utilisés par l'entreprise. Cela concerne les ordinateurs, smartphones, tablettes, mais également les périphériques tels que les imprimantes, ou tout autre objet ou machine connecté au réseau ou à Internet.
- Créez et partagez une politique de cybersécurité pour l'entreprise qui prend en compte :
  - Les rôles, responsabilités et accès de chaque collaboratrice et collaborateur, ainsi que de tout tiers – personne ou entreprise – qui pourrait accéder à des informations sensibles.
  - La marche à suivre pour se protéger contre les attaques et pour limiter les dommages si cela arrive.

2 Protéger

- Contrôlez qui peut accéder au réseau de votre entreprise et qui peut utiliser les ordinateurs et autres appareils (collaboratrices, collaborateurs, clientes et clients, partenaires, prestataires).
- Utilisez et configurez des logiciels de sécurité pour protéger vos données.
- Chiffrez les données sensibles et conservez les clés de chiffrement dans un lieu sûr et séparé.
- Définissez un plan de sauvegarde régulier et automatisé de vos données (voir pages 15-16).
- Mettez à jour régulièrement ou automatisez les mises à jour de tous vos logiciels.
- Formez régulièrement toutes les personnes qui utilisent vos équipements. Aidez vos collaboratrices et collaborateurs à comprendre les enjeux et les risques pour eux-mêmes et pour l'entreprise.

3 Détecter

- Mettez en place une surveillance active de vos équipements pour détecter tout accès non autorisé par des personnes, des périphériques (comme des clés USB) et des logiciels.
- Surveillez les connexions non autorisées à votre réseau.
- Menez une investigation pour toute activité suspecte sur votre réseau et vos systèmes.

Établir une stratégie

4 Répondre

Etablissez un **Plan de continuité des activités (PCA)** pour que vous puissiez, en cas d'interruption de service et/ou d'attaque :

- Identifier et contenir l'attaque.
- Signaler l'attaque aux autorités compétentes.
- Avertir vos clientes et clients, vos équipes et partenaires dont les données pourraient avoir été exposées.
- Assurer la continuité de vos activités.
- Résorber les failles et rétablir l'activité.
- Mettre à jour votre politique de gestion des cyber-risques.
- Anticiper d'éventuels scénarios imprévus (comme un incident naturel) qui pourraient endommager vos données.

Testez et mettez régulièrement à jour votre PCA

5 Restaurer

Après une attaque :

- Identifiez, répertoriez et analysez les dommages causés (équipements endommagés, fuite de données, accès compromis, etc.).
- Sécurisez et assainissez votre environnement de travail et les équipements qui ont été impactés.
- Réparez et restaurez les équipements et les parties de votre réseau qui ont été endommagés.
- Tenez informés vos équipes, clientes et clients et partenaires de l'avancée des démarches de restauration.

Pour vous aider à établir une stratégie de protection contre les cyber-risques et la mettre en place, faites-vous accompagner par une entreprise spécialisée.

Le saviez-vous?

En cas de cyber-attaque, la durée moyenne pour une restauration complète du fonctionnement de l'entreprise est de 22 jours.

Pour aller plus loin, consultez le site Internet de l'**Office fédéral de la cybersécurité (OFCS)** de la Confédération.

Sécurité physique des ressources numériques

La prévention des cyber-risques commence avec la sécurité physique

Des lacunes dans la sécurité physique peuvent exposer des données sensibles.

Par exemple :

- Un ordinateur ou un téléphone portable non sécurisé oublié dans le train.
- Des documents d'archives déposés dans un point de collecte des déchets, accessibles à toutes et tous.
- Des dossiers et du matériel informatique dérobés lors d'un cambriolage.

Responsabilité numérique des entreprises

Sensibiliser ses collaboratrices et collaborateurs à la responsabilité numérique est essentielle car ils sont souvent le maillon le plus vulnérable face aux cyber-menaces, et leurs actions peuvent directement impacter la sécurité et la réputation de l'entreprise.

Consultez le guide sur la responsabilité numérique des entreprises.

Comment protéger vos équipements et vos dossiers physiques

- Stockez de manière sécurisée vos dossiers papier et équipements électroniques contenant des informations sensibles dans une armoire ou une pièce fermée, résistant aux incendies (faites appel à des entreprises spécialisées).
- Limitez l'accès à vos archives, dossiers ou équipements aux personnes autorisées et conservez une trace de tous ces accès.
- Détruisez de manière sécurisée les dossiers et données obsolètes. Utilisez un destructeur de documents ou faites appel à une entreprise spécialisée dans la destruction sécurisée pour éliminer les documents papier ou les supports de données. Ne vous contentez pas de les jeter ou de les recycler.
- Rappelez régulièrement à vos équipes de verrouiller leur poste de travail lorsqu'ils s'absentent et de ne pas laisser sans surveillance des documents sensibles, clés USB, disques durs, téléphones portables, etc.
- Demandez à vos équipes de sécuriser leurs smartphones selon les bonnes pratiques en vigueur s'ils en font un usage professionnel.

Sécurité physique des ressources numériques

Comment sécuriser l'accès à vos appareils

La perte, le vol ou la mauvaise utilisation d'un appareil peut avoir de graves conséquences.

Sécurisez les données contenues dans ces appareils en appliquant les bonnes pratiques suivantes :

- Utilisez des mots de passe forts : un mot de passe robuste est long (12 caractères minimum), complexe et unique (contenant des caractères spéciaux tels que !?@#%, des lettres majuscules et minuscules et des chiffres).
- Assurez-vous que ces mots de passe soient générés et stockés de manière sécurisée, en utilisant un gestionnaire de mots de passe.
- Définissez un mot de passe différent pour chaque compte ou application.
- Différenciez les mots de passe privés des mots de passe professionnels.
- Ne communiquez jamais vos mots de passe.
- Changez régulièrement vos mots de passe.
- Verrouillez vos appareils au moyen de codes.
- Imposez l'authentification multifacteur (MFA) pour accéder à votre réseau d'entreprise et à ses différents outils (ex : mot de passe à usage unique et/ou double authentification).
- Désactivez bluetooth de vos appareils lorsque vous n'en avez pas besoin.
- Limitez les tentatives de connexion à 5 maximum pour vous protéger des intrusions.
- Chiffrez vos appareils mobiles contenant de l'information sensible. Chiffrez également les échanges internes ou externes contenant des informations sensibles.
- Entreposez vos clés de cryptage en lieu sûr et séparé de vos infrastructures.
- Avant de revendre ou de donner d'anciens ordinateurs, appareils mobiles, imprimantes ou autres équipements électroniques, utilisez un logiciel de destruction de données ou faites appel à une entreprise spécialisée. Ne vous contentez pas d'effacer simplement les données.
- Informez régulièrement vos équipes sur les cyber-risques et formez-les en mettant à leur disposition le matériel adéquat ainsi que des possibilités de formation continue.
- Encouragez l'adoption de bonnes pratiques en matière de sécurité, que ce soit au bureau ou à la maison.
- Diffusez votre **plan de continuité des activités (PCA)**. Chaque membre de l'équipe doit savoir qui contacter, et connaître les étapes à suivre si un équipement ou un dossier est perdu ou volé.

Sécuriser les accès à distance

Vos équipes et partenaires doivent suivre des standards de sécurité élevés lorsqu'ils accèdent à distance à votre réseau, qu'il s'agisse des équipements de votre entreprise ou d'équipements personnels.

Protéger les équipements lors d'un accès à distance

- Sécurisez votre routeur : changez systématiquement les paramètres par défaut (nom et mot de passe), et maintenez le logiciel à jour.
- Chiffrez par défaut les données qui transitent sur les réseaux ou se trouvant sur les appareils qui se connectent à votre réseau à distance.
- Paramétrez les réglages des smartphones, tablettes et ordinateurs portables : changez les réglages par défaut pour empêcher les connexions automatiques aux réseaux sans fil.
- Maintenez à jour les logiciels anti-virus et programmez des mises à jour automatiques sur tous les équipements susceptibles de se connecter à distance à votre réseau (ordinateurs et appareils mobiles inclus).

Télétravail

Lorsque vous êtes à l'extérieur de l'entreprise, respectez les règles établies par votre entreprise concernant l'utilisation des outils informatiques et de sécurité. Appliquez également les bonnes pratiques de cyber-sécurité à votre domicile et en déplacement.

Fournir aux équipes et partenaires des outils qui permettent de maintenir un haut niveau de sécurité

- Assurez-vous que tout accès depuis un emplacement extérieur passe par un routeur appliquant les meilleurs standards en matière de chiffrage des communications sans fil (tels que WPA2 ou WPA3).
- Utilisez un VPN d'entreprise pour permettre à vos équipes d'accéder à distance à votre réseau, afin de chiffrer le trafic entre les appareils et le réseau Internet.
- Mettez en place l'authentification multifacteur (MFA) et l'utilisation de mots de passe robustes.
- Assurez-vous que le réseau Wi-Fi pour les invités est bien séparé du réseau de l'entreprise et fournir des codes de connexion uniques pour les invités.
- Incluez des clauses de sécurité dans tous les contrats avec les partenaires qui doivent se connecter au réseau de l'entreprise.

Hébergement Web

Vous souhaitez créer un site Internet ou le mettre à jour ?

Si vous ne disposez pas des compétences nécessaires pour mettre en place un site Internet, faites appel à un spécialiste en création et hébergement de sites Internet. Il existe de nombreuses options d'hébergement web, qu'il conviendra d'étudier en fonction de vos besoins. Lors de la comparaison des services, la sécurité doit être une préoccupation centrale.

Les questions à poser à votre futur prestataire

- ☐ Le site est-il sécurisé par un protocole TLS, et est-ce inclus dans le contrat d'hébergement ?
- ☐ Je souhaiterais utiliser mon nom de domaine pour mes adresses e-mail professionnelles, pouvez-vous mettre en place un mécanisme de sécurité, tel que SPF, DKIM ou DMARC ?
- ☐ Qui est responsable des mises à jour de sécurité et de la maintenance de mon site Internet et à quelle fréquence sont-elles effectuées ?
- ☐ Une fois que le site Internet est en ligne, qui aura les droits d'administration et d'édition ?
- ☐ Une authentification multifacteur sera-t-elle mise en place pour les personnes qui auront les droits d'administration et d'édition du site Internet ?

Sécurisez votre site Internet à l'aide de TLS

TLS est un protocole de sécurité conçu pour fournir des communications sécurisées sur un réseau informatique. Il est utilisé pour chiffrer les données transmises sur le réseau, garantissant ainsi la confidentialité et l'intégrité des informations échangées entre deux systèmes. Lorsque TLS est correctement mis en place sur votre site Internet, votre URL commencera par http**s**://.

Authentifiez vos adresses e-mail

Vous pouvez configurer les adresses e-mail de votre entreprise pour qu'elles utilisent le nom de domaine de votre site Internet (par exemple : masociete.ch / nom@masociete.ch). Afin de s'assurer que des escrocs ne puissent pas envoyer des e-mails en votre nom en usurpant le nom de domaine de votre organisation, vous devez certifier l'authenticité des e-mails. Pour ce faire, vous pouvez vous appuyer sur des mécanismes ou des normes de vérification comme Sender Policy Framework (SPF), Domaine Keys Identified Mail (DKIM), Domain-based Message Authentification, Reporting & Conformance (DMARC).

Assurez la maintenance de votre site Internet

Il est nécessaire de clarifier dès le départ qui est responsable de la maintenance du site Internet. Celle-ci peut être effectuée à l'interne ou par un prestataire externe, selon les compétences dont vous disposez. Assurez-vous d'une mise à jour régulière des composants du site Internet et de la sécurité.

Assurances et aspects juridiques

Gérer un cyber-incident et remettre son entreprise en état de fonctionnement est coûteux et complexe

Il existe des offres de cyber-assurances à destination des PME en Suisse qui peuvent comprendre une assistance technique, une protection contre les pertes financières, une couverture de la responsabilité civile et une assistance juridique. Souscrire à une assurance ne vous dédouane pas et ne vous protège pas contre un cyber-incident.

Check-list avant de souscrire à une cyber-assurance :

- ☐ Le site est-il sécurisé par un protocole TLS, et est-ce inclus dans le contrat d'hébergement ?
- ☐ Faire une étude des activités de l'entreprise afin d'établir un inventaire des risques auxquels elle est le plus exposée en fonction du niveau d'impact.
- ☐ Déterminer l'étendue de la couverture dont l'entreprise a besoin.
- ☐ Évaluer les différentes options d'assurance et choisir celle qui répond le mieux aux besoins de l'entreprise en fonction de ses activités.
- ☐ S'informer sur les couvertures et les exclusions de chaque police.
- ☐ Se renseigner sur les risques couverts par l'assurance, notamment la perte de données, les réclamations de renseignements personnels, les violations de données et les frais juridiques et professionnels engendrés par des violations par un tiers.
- ☐ S'assurer que la police d'assurance couvre bien les risques auxquels l'entreprise pourrait être exposée et que l'indemnisation correspond au niveau de risque assuré.

Pour vous aider dans votre évaluation des risques, consultez la plateforme de l'**Observatoire du Numérique**.

Cadre légal

En Suisse, la gestion des cyber-risques s'inscrit dans le cadre légal régis par la loi sur la sécurité de l'information (LSI) et la loi sur la protection des données (LPD).

Les cadres réglementaires varient selon les régions et le type d'activité des entreprises. Il est indispensable de se renseigner sur les réglementations en vigueur dans les pays dans lesquels l'entreprise est active afin d'être en conformité avec les lois en vigueur.

Pour plus d'informations, consultez le guide **Réglementations relatives à la protection des données dans le monde**

Le saviez-vous?

Selon l'article 19 de la Loi fédérale sur la protection des données (LPD), vous êtes tenu d'informer les personnes lorsque vous collectez des données les concernant.

Le phishing ou hameçonnage

Comment ça marche?

Vous recevez un e-mail ou un message texte

Il semble provenir d'une personne ou d'une entreprise que vous connaissez, qui vous demande de répondre par e-mail ou en cliquant sur un lien afin de lui fournir des détails sur votre identité, votre mot de passe, ou encore des informations sensibles sur l'entreprise.

Ça a l'air authentique

Il est facile de falsifier des logos et de créer de fausses adresses e-mail. En général, les fraudeurs utilisent des noms d'entreprise familiers ou se font passer pour des personnes que vous connaissez.

C'est urgent

L'expéditeur vous incite à agir rapidement ou dans l'urgence, laissant penser que des conséquences négatives se produiront si vous n'agissez pas.

Ce qui se passe ensuite

Si vous cliquez sur un lien, les pirates peuvent identifier que vous avez interagi avec le message et poursuivre la sollicitation dans le but de vous soutirer des informations ou vous inciter à effectuer des actions, comme un versement d'argent.

Si vous recevez un message qui vous paraît suspect …

- **Vérifiez l'adresse de l'expéditeur**
- **Vérifiez les URL en les survolant avec la souris avant de cliquer dessus**
- **Ne répondez pas à ce message**
- **Ne révélez jamais votre identité**
- **Ne communiquez jamais de coordonnées bancaires**
- **Ne versez jamais d'argent**
- **N'ouvrez pas les pièces jointes**

*Annoncez les messages frauduleux sur la plateforme de l'**Office fédéral de la cybersécurité (OFCS):** https://www.ncsc.admin.ch/*

Signalez-le !

Si vous avez reçu un e-mail de phishing ou découvert un site de phishing, annoncez-le sur **https://antiphishing.ch**

Testez vos équipes !

Effectuez régulièrement des tests à l'interne pour évaluer la conscience et la compréhension des collaboratrices et collaborateurs vis-à-vis des cyber-risques et enjeux pour l'entreprise, par exemple au moyen d'une campagne de faux hameçonnage.

Cas pratiques

Il suffit d'un clic…

Lorsqu'une personne clique sur un lien frauduleux qui permet d'installer un ransomware, tout le réseau de l'entreprise se bloque et les données sont prises en otage. Les pirates demandent une rançon, sous forme de virement bancaire ou de cryptomonnaie, pour débloquer l'accès aux données. Entre-temps, l'activité de l'entreprise est bloquée. Les données nécessaires à son fonctionnement, les renseignements sensibles sur la clientèle, les équipes et les activités commerciales se retrouvent entre les mains des pirates informatiques.

Près de 80% des cyber-incidents résultent d'une erreur humaine interne à l'entreprise ou liées à ses partenaires.

L'Office fédéral de la cybersécurité (OFCS) recommande de procéder à une dénon-ciation pénale dans tous les cas. Prenez contact avec la police cantonale. Vous pouvez trouver le poste de police compétent le plus proche sur le site Internet ***« Suisse e-Police »***.

Les virus informatiques, comment ça marche ?

Il y a plusieurs moyens d'implanter des logiciels malveillants dans un système :

- Par l'intermédiaire d'e-mails frauduleux contenant des liens ou des pièces jointes qui mettent vos données et votre réseau en danger. Ces emails d'hameçonnage (ou phishing – voir page précédente) sont à l'origine de la plupart des attaques avec demande de rançon (ou ransomware).
- En visitant des sites Internet infectés, en scannant un qr-code ou en cliquant sur des liens qui téléchargent automatiquement un logiciel malveillant sur votre ordinateur ou votre smartphone.
- En connectant un périphérique ou un ordinateur externe à l'entreprise sur votre réseau ou sur vos ordinateurs (clé USB, disque dur, smartphone etc.).
- En exécutant des applications non vérifiées ou non approuvées.
- En autorisant l'ouverture de liens externes ou le lancement de macros lors de l'accès à des documents qui vous sont transmis par une personne extérieure à l'organisation.

Que faire en cas de demande de rançon?

L***'OFCS*** déconseille de payer une rançon, car vous n'aurez aucune garantie que vos données vous seront rendues. De plus, céder au chantage contribue à financer les activités criminelles et encourage les criminels à poursuivre leurs activités ou à recommencer.

Prévenir les attaques et leurs conséquences

Etablissez un plan de continuité des activités (PCA)

Ce plan vous permettra de maintenir votre entreprise en activité dans le cas d'une cyber-attaque ou d'un cyber-incident. Mettez ce plan par écrit, communiquez-le à l'interne et testez-le régulièrement.

Sensibilisez vos équipes à l'ingénierie sociale

Formez et informez vos équipes sur les différentes techniques de manipulation utilisées pour inciter une personne à transmettre elle-même des informations, qu'elles soient sensibles ou non. Ces données peuvent être des renseignements personnels ou des informations confidentielles permettant d'accéder au réseau informatique d'une organisation. Les techniques utilisées consistent à exploiter le facteur humain, par exemple en usurpant l'identité ou le rôle d'une personne ou d'une organisation.

Avant de cliquer sur un lien douteux …

- Vérifiez que le nom de domaine existe vraiment et qu'il correspond à ce que vous souhaitez consulter.
- Vérifiez que le site est sécurisé : l'URL doit commencer par https (le « s » de « http**s** » indiquant que les informations sont chiffrées), et contrôlez que le certificat ne soit pas expiré ou invalide (le cadenas à côté de l'URL ne doit pas être barré).
- Assurez-vous que vous vous adressez à une personne ou une organisation réelle et digne de confiance, et que vous n'êtes pas sur le point de télécharger un logiciel malveillant ou de partager vos accès avec un escroc.
- En cas de doute, parlez-en autour de vous. Cela vous aidera à déterminer si la demande est réelle ou s'il s'agit d'une tentative d'hameçonnage.
- Si le doute persiste, téléphonez directement au fournisseur concerné ou à la personne qui est censée vous avoir envoyé le mail. Méfiez-vous du numéro qui figure dans le message et préférez votre répertoire.

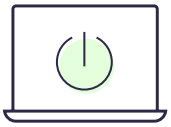
Soyez proactifs !

Le saviez-vous?

En cas de cyber-attaque, la durée moyenne pour une restauration complète du fonctionnement de l'entreprise est de 22 jours.

Marche à suivre en cas d'attaque

1 Limitez les dommages



- Coupez les réseaux internes (Wi-fi et LAN) et externe (WAN / Internet).
- Identifiez l'ordinateur ou les appareils infectés et éteignez-les. Si vous ne parvenez pas à rapidement les identifier, effectuez ces opérations pour l'ensemble du parc informatique.
- Modifiez tous les mots de passe.
- Effectuez ou faites effectuer un contrôle de tous les appareils (ordinateurs et serveurs) pour s'assurer qu'ils ne sont pas infectés.

2 Donnez l'alerte

- Suivez les procédures mises en place par l'entreprise pour avertir votre responsable ou prestataire IT.
- Alertez vos collègues et partagez votre expérience en cas de phishing, car ces tentatives concernent souvent plus d'une personne au sein d'une entreprise.

3 Signalez la fraude

- Si des données ou renseignements personnels ont été compromis, avertissez les personnes concernées.
- Annoncez les messages frauduleux sur la plateforme de l'***Office fédéral de la cybersécurité (OFCS)***.
- Portez plainte auprès de la police en cas d'infraction.

4 Communiquez

- Tenez informés vos collaboratrices, collaborateurs, partenaires, clientes et clients.

Référez-vous à la loi fédérale sur la sécurité de l'information (LSI)*
L'article 74b liste les autorités et organisations assujetties à l'obligation de signaler une cyber-attaque. De nombreuses entreprises dans différents secteurs sont concernées.

Proposition de stratégie de sauvegarde des données

La sauvegarde, ou backup, consiste à dupliquer sur un support et/ou un espace externe les informations nécessaires au bon fonctionnement de l'entreprise, et à les mettre en sécurité pour pouvoir y accéder en cas de cyber-incident. Sans sauvegarde, il est impossible de restaurer les données de l'entreprise.

Mise en place d'un plan de sauvegarde

1

Cartographiez les données

- Faites un inventaire de toutes les données que vous possédez.
- Évaluez la criticité des données pour l'activité de l'entreprise.
- Organisez et catégorisez ces données.
- Définissez l'emplacement des données : recensez les équipements qui les utilisent et les emplacements où elles sont stockées.
- Répertoriez les personnes et les systèmes ayant accès à ces données.

2

Hiérarchisez les données

Classez vos données par niveau d'importance. Pour cela, posez-vous les questions suivantes :

- Quels sont les fichiers et informations indispensables au fonctionnement global de l'organisation et à chacun de ses services ou départements ? (par exemple : comptabilité, contacts, fiches clients, agendas, RH, documents stratégiques et commerciaux, etc.).
- Quelles sont les données et documents indispensables et non-récupérables en cas de perte, de vol ou de destruction du matériel ?

3

Définissez des emplacements de sauvegarde

Pour une bonne stratégie de sauvegarde et une restauration rapide des données de l'entreprise, sauvegardez vos données à 3 endroits différents :

- **Stockage sur une solution de sauvegarde au sein de l'organisation (ex : serveur de backup)**
- **Stockage hors-ligne sur un disque dur, au sein de l'organisation et accessible rapidement (ex : pièce sécurisée)**
- **Stockage sur un disque entreposé en-dehors de l'organisation (ex : coffre en banque)**

Pour plus de sécurité et d'autonomie, vous pouvez effectuer une sauvegarde supplémentaire sur un NAS (mini serveur de fichiers), un SAN (solution de sauvegarde adaptée aux moyennes et grandes entreprises), un cloud ou un data center.

En cas de stockage dans un cloud, faites attention à l'endroit où sont situés les serveurs qui hébergent les données, aux obligations légales de l'entreprise en matière d'hébergement des données, et aux législations qui s'appliquent selon les pays. Il est recommandé de privilégier l'usage d'un cloud qui stocke et traite les données sur le territoire national.

Proposition de stratégie de sauvegarde des données

4 Mettez en place un calendrier de sauvegarde

Il est important de sauvegarder régulièrement les données. Déterminez une fréquence adaptée aux activités de votre organisation.

Par exemple, vous pouvez mettre en place une sauvegarde quotidienne, complétée par des sauvegardes hebdomadaires et mensuelles. Contrôlez et testez régulièrement les archives de sauvegarde ainsi que les processus de restauration.

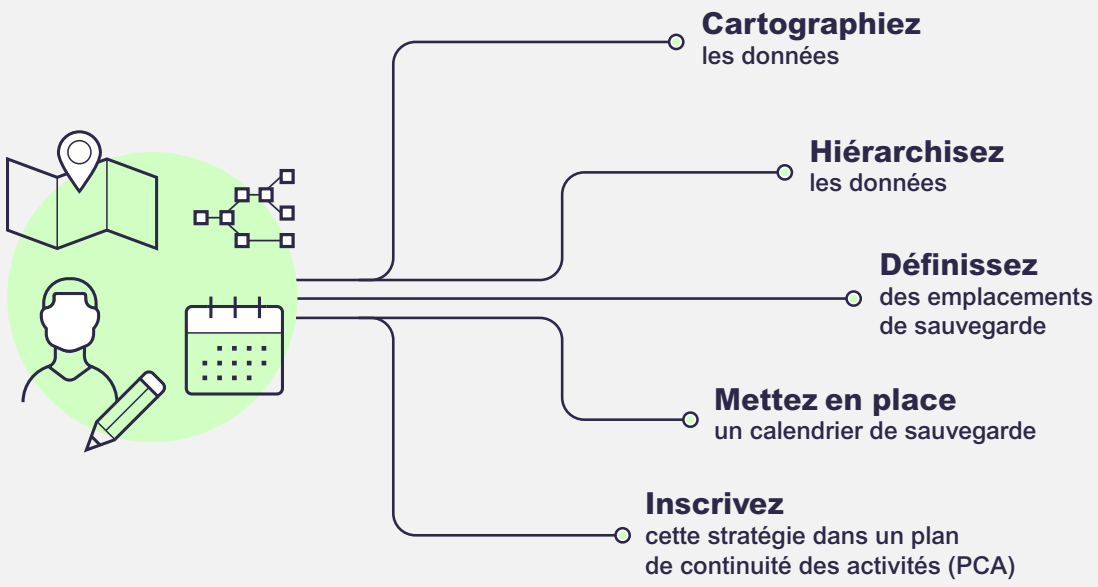
Ce calendrier vous permettra de restaurer facilement et rapidement vos données en cas d'incident, avec une perte minimale, voire inexistante.

5 Inscrivez cette stratégie dans un plan de continuité des activités (PCA)

Le PCA décrit comment maintenir la continuité de vos activités afin de minimiser les interruptions et les perturbations opérationnelles (voir page 5). Il établit entre autres la marche à suivre pour sécuriser et restaurer les données en cas d'incident informatique.

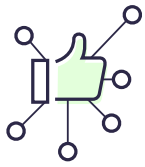
La stratégie de sauvegarde en constitue donc une partie essentielle, puisqu'elle détermine la manière dont le service informatique peut être remis en service pour relancer les activités.

Plan de sauvegarde



En bref

Mauvaises pratiques



- Croire que la cyber-sécurité est uniquement un problème informatique.
- Adopter une nouvelle technologie et de nouvelles pratiques numériques sans analyse préalable des risques et opportunités.
- Sous-estimer le risque d'impact ou la probabilité d'un cyber-incident.
- Négliger l'importance d'un plan de continuité et d'une stratégie de sauvegarde des données.
- Collecter et traiter plus d'information que nécessaire.

Bonnes pratiques pour protéger vos équipements, votre réseau et vos données

- Maintenez vos logiciels à jour.
- Sécurisez votre routeur wifi par un cryptage WPA2 ou WPA3.
- Sauvegardez régulièrement vos données.
- Exigez des mots de passe forts et uniques pour tous les équipements et accès.
- Activez une authentification multifacteur.

Bonnes pratiques pour protéger votre personnel, votre entreprise, vos clientes et clients et vos partenaires

- Établissez une politique où l'accès aux ressources est restreint par défaut et n'est autorisé qu'aux personnes concernées.
- Limitez les informations publiées sur votre site d'entreprise. Evitez toute information permettant d'identifier des personnes et leur rôle au sein de l'entreprise, afin de prévenir toute usurpation d'identité ou manœuvre d'ingénierie sociale.
- Formez vos équipes en mettant à leur disposition du matériel adéquat ainsi que des possibilités de formation continue interne ou externe.

La sécurité de votre entreprise est primordiale !
Faites-vous accompagner par des spécialistes.