cpme BRETAGNE

TRAVAIL À DISTANCE : PRÉVENIR LES ACTES DE CYBER MALVEILLANCE

FICHE PRATIQUE

TRAVAIL À DISTANCE : PRÉVENIR LES ACTES DE CYBERMALVEILLANCE

Le travail à distance ou *nomadisme numérique* n'a cessé de prendre de l'ampleur ces dernières années et fait partie intégrante des pratiques de nombreux chefs d'entreprise et de salariés.

Depuis mars 2020, en raison de la crise de la Covid-19, de nombreuses activités ont été obligées de revoir leur organisation et de mettre en place des formes de travail à distance, souvent dans l'urgence et en l'absence d'accord d'entreprise sur le télétravail.

Cette augmentation croissante du travail à distance pose donc la question des moyens de sécurisation des données stratégiques des entreprises dans un contexte où les actes de cyber malveillance et les cyberattaques ont explosé, fragilisant de nombreuses TPE-PME.

À travers cette fiche pratique, nous vous donnons des conseils pour faire preuve de vigilance dans votre entreprise.

UNE AUGMENTATION GRANDISSANTE DES LIEUX DE CONNEXION

Les situations de travail à distance sont multiples : réunion chez un client ou un prestataire, travail dans les transports en commun (train, bus, métro…), travail régulier ou ponctuel dans un espace de coworking, dans un centre d'affaires ou un hôtel, dans des lieux publics (médiathèques, bibliothèques…) ou travail ponctuel à domicile pour des raisons personnelles (garde d'enfant notamment…).

Ainsi, **le lieu de connexion du travailleur nomade peut présenter des niveaux de sécurité variables** selon l'environnement et peut être source d'acte de cyber malveillance (ex : wifi public piraté avec un risque d'usurpation de données). Il est donc essentiel de pouvoir adopter de bons réflexes et intégrer certaines bonnes pratiques pour garantir une sécurité optimale de ses données et ne pas mettre en péril les données stratégiques de l'entreprise, même à distance.

MAXIMISER LA SÉCURITÉ DE L'ENTREPRISE ET LA PROTECTION DE SES DONNÉES À DISTANCE

La protection des données de l'entreprise dépend beaucoup de vos choix en termes d'infrastructure, d'équipement Informatique et de logiciels.

Mais **la sécurité est l'affaire de tous**. Il est important d'**impliquer l'ensemble de ses collaborateurs et prestataires** dans la protection de l'entreprise et de pouvoir, en cas d'incident ou de suspicion d'incident, récupérer l'activité de l'ensemble des équipements.

Intégrer des réflexes de sécurité informatique à ses pratiques courantes et encadrer les pratiques de vos salariés et prestataires dans leur travail à distance sont autant de moyens de vous aider à maximiser la protection de votre entreprise.

1. VÉRIFIER QUE LES ÉQUIPEMENTS DE VOS SALARIÉS SONT CORRECTEMENT PROTÉGÉS

Pour protéger les données de l'entreprise (annuaire-clients, messagerie…), nous vous recommandons d'équiper l'ensemble des postes de travail (ordinateurs, smartphones, tablettes) **d'un pare-feu, d'un anti-virus et d'un outil de blocage d'accès aux sites malveillants**.

L'utilisation d'un VPN permettant d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur est également recommandée.

✔ Pour vous accompagner, l'Agence Nationale de la Sécurité des Systèmes d'Information met à votre disposition une liste de logiciels et matériels ayant reçu une qualification de sécurité.

Par ailleurs, nous vous rappelons qu'il est essentiel de réaliser des **mises à jour régulières** de l'ensemble des applications et anti-virus installés sur les différents équipements. En cas de téléchargement de logiciels ou d'applications, veillez à ce qu'ils soient téléchargés sur les **sites officiels des éditeurs** pour plus de sécurité.

2. ENCADRER L'ACCÈS AUX DOCUMENTS STRATÉGIQUES ET AUX DONNÉES SENSIBLES

La structure d'une entreprise évolue dans le temps. Les équipes sont amenées à s'agrandir ou à changer (arrivée et départ de stagiaires, de collaborateurs, départ à la retraite…).

Que vous ayez ou non un turn-over important dans votre entreprise, il est important que vous puissiez **contrôler et limiter le nombre de services mis à disposition de vos équipes au strict minimum**, pour limiter les risques d'actes de cyber malveillance.

Vous pouvez mettre en place des **restrictions d'utilisation de certaines applications** ainsi que des **mécanismes d'authentification à double facteur sur les services accessibles à distance** pour limiter les risques d'intrusion.

✔ La **double authentification** permet d'accéder aux services après avoir apporté deux preuves d'identité (comme par exemple la saisie d'un code reçu par sms sur votre téléphone, après avoir renseigné votre identifiant et votre mot de passe).

3. VÉRIFIER QU'UNE JOURNALISATION DE L'ACTIVITÉ EST MISE EN PLACE

Les journaux sont une source d'information riche pouvant être utilisée pour détecter des incidents de sécurité ou retrouver des traces d'un incident de sécurité. **Nous vous conseillons de vérifier auprès de vos prestataires informatiques qu'une journalisation existe pour l'ensemble de vos équipements.**

Le but est de pouvoir retracer toute l'activité d'un réseau et d'apporter la preuve de cette activité (utilisation ou non-utilisation d'une application ou d'un service par un utilisateur, accès illégitime d'un utilisateur à une ressource...).

En effet, **l'absence de journaux rendra difficile la détection d'incidents et l'élaboration d'un diagnostic et pourra constituer une infraction**.

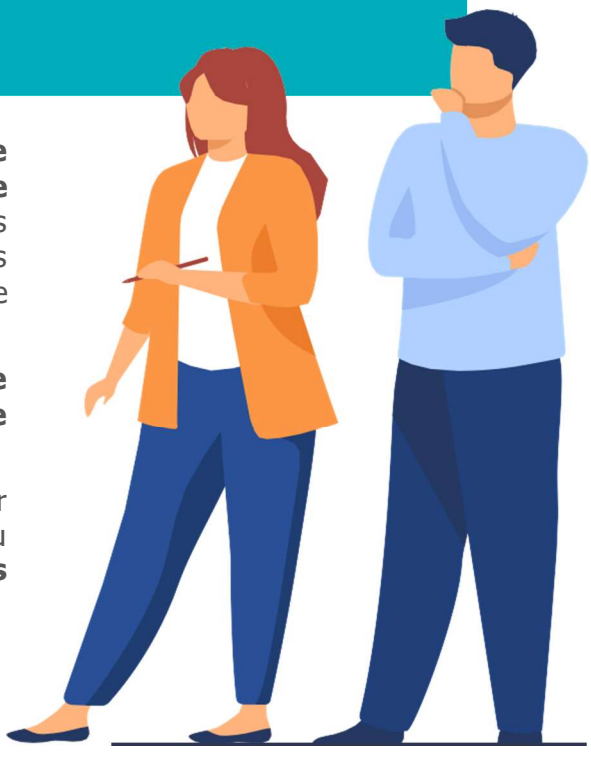
✔ Pour être opposable en cas de contentieux, la journalisation doit respecter les règles relatives à l'administration de la preuve et les principes directeurs des procès civils et pénaux (loyauté, intégrité, licéité, etc.).

✔ L'Article 226-17 du Code pénal prévoit que **« Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques (sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement »**. En cas d'attaque, si un manquement à cette obligation de sécurité est avéré, alors **la responsabilité pénale peut être engagée** et les sanctions encourues sont lourdes : **jusqu'à 5 ans d'emprisonnement et 300 000 euros d'amende.**

Par ailleurs, **réaliser une sauvegarde régulière des données vitales de l'entreprise** et posséder une copie de ces dernières vous permet de réagir plus rapidement en cas d'incident ou de cyberattaque.

La sauvegarde de vos données est **une condition de la continuité de votre entreprise**.

Aussi, il est important de pouvoir les stocker sur des équipements déconnectés de votre réseau principal, de **vérifier que ces sauvegardes sont bien réalisées**, et qu'elles fonctionnent.



4. PRENDRE LE TEMPS DE SENSIBILISER VOS COLLABORATEURS AUX RISQUES INFORMATIQUES

Votre entreprise peut être confrontée à des actes de cyber malveillance (interne et externe). Cependant, **la sensibilisation de vos collaborateurs peut vous aider à vous en prémunir** car, eux aussi, y sont confrontés dans leur quotidien (réception de mails frauduleux, réception de faux ordres de virement…).

Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. À ce titre et **dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité** des systèmes d'information à travers des actions de sensibilisation et de formation.

✔ Dans le cadre d'un déplacement domicile-travail ou dans le cadre de rendez-vous professionnels réguliers hors de votre entreprise, mettez à leur disposition des filtres écran de confidentialité qui permettent de restreindre la vision des données affichées sur l'écran de leur ordinateur, de leur tablette ou de leur smartphone.

Insistez, en interne, sur **le renforcement du niveau de sécurité des mots de passe en privilégiant une authentification forte** : mot de passe suffisamment long et complexe, utilisation d'un gestionnaire de mot de passe permettant de générer et de gérer vos mots de passe de façon sécurisée… et **un changement régulier**.

Enfin, il est primordial de veiller à ce que vos équipes pratiquent **une séparation stricte des usages de leurs ordinateurs et tablettes** : usage professionnel et usage personnel ne doivent pas se mélanger car cela pourrait compromettre certaines données stratégiques de l'entreprise.

5. FAIRE REMONTER TOUTE SUSPICION D'INCIDENT OU TOUT INCIDENT

À la réception d'un faux ordre de virement ou bien d'une suspicion de faux, d'un mail frauduleux reprenant les codes et couleurs d'un site institutionnel (URSSAF, site des impôts…), il est important de le signaler afin d'éviter de vous faire arnaquer, de vous faire usurper votre identité et ainsi éviter à d'autres d'en être victimes.

Alertez **votre gendarmerie la plus proche, votre prestataire informatique** ainsi que des acteurs tels **l'ANSSI, Cybermlaveillance.gouv.fr**, etc.

En cas de suspicion ou d'incident, le mot-clé à retenir : réactivité.

✔ Conservez des preuves de ces incidents (capture d'écran de votre ordinateur, mail avec les liens dit frauduleux…)

✔ Listez l'ensemble des préjudices subis

✔ Munissez-vous de tout élément qui vous semble pertinent

✔ Portez plainte auprès des services de Police ou de Gendarmerie

Bonnes pratiques

✔ Adopter une politique de mot de passe rigoureuse ;

✔ Sauvegarder ses données régulièrement ;

✔ Faire ses mises à jour régulièrement ;

✔ Se protéger des virus et autres logiciels malveillants (Anti-virus gratuit à éviter, il est intéressant d'opter pour une suite de sécurité) ;

✔ Éviter les réseaux WIFI publics

✔ Séparer les usages professionnels et personnels, surtout avec la pratique exponentielle du télétravail

✔ Éviter de naviguer sur des sites douteux ou illicites et être vigilant lors du téléchargement d'un fichier

✔ Contrôler les permissions des comptes utilisateurs

✔ Être très vigilant avec les liens ou les pièces jointes contenus dans les messages électroniques

✔ Faire attention aux informations personnelles ou professionnelles que vous diffusez sur Internet

✔ En cas de ransomware, ne jamais payer de rançon !

✔ En cas de doute ou de fait avéré, contacter la gendarmerie et déposer plainte

Face à l'évolution des pratiques de travail et à un recours plus régulier au travail à distance, il est judicieux pour la pérennité d'une entreprise d'intégrer une démarche de cybersécurité dans sa stratégie.

Nos conseils pratiques

✔ Dialoguez avec votre prestataire informatique si vous en avez un ;

✔ Sensibilisez vos collaborateurs aux bonnes pratiques ;

✔ Faites des mises à jour régulières de vos outils informatiques ;

✔ Adoptez vos pratiques et bons réflexes informatiques aux besoins de votre activité ;

✔ Faites-vous accompagner si nécessaire par l'ANSSI, la Gendarmerie, la Police, Cybermalveilllance.gouv.fr… ;

✔ Des questions, des interrogations ? Contactez votre CPME.

Pour plus d'informations

Consultez le « Guide de recommandations sur le nomadisme numérique » rédigé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Pourquoi ce guide ?

Dans le cadre Mois européen de la cybersécurité (Cybermoi/s), déclinaison française de la campagne *European CybserSecurity Month,* la CPME Bretagne se mobilise et vous propose ce guide, suite au Webinaire que nous avions organisé au côté de la Gendarmerie des Côtes d'Armor, afin de vous permettre de mieux « cyber sécuriser » votre entreprise.

www.cpme-bretagne.fr
06 47 87 63 87 – contact@cpme-bretagne.fr