RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

LA CYBERSÉCURITÉ POUR LES TPE/PME EN 12 QUESTIONS

SOMMAIRE

AVANT-PROPOS

En réduisant les coûts de certains investissements, en optimisant les processus et en rapprochant les entreprises de leurs clients, leurs partenaires ou encore des services publics, la numérisation apporte d'incroyables opportunités aux TPE et aux PME. Il n'est désormais plus question de se passer des bénéfices formidables de ces nouveaux outils.

Mais cette transformation s'accompagne de risques réels qui ne cessent de s'intensifier, le nombre d'attaques informatiques augmentant de façon dramatique. Vol de données, demandes de rançon, atteinte à l'image ou sabotage sont autant de risques qui pèsent sur les organisations, avec des conséquences souvent graves, parfois irréversibles.

Cette réalité peut encore sembler abstraite, très technique, complexe et coûteuse pour les entreprises, notamment les plus petites, si bien qu'elles ne se préparent pas toujours suffisamment. Les conséquences sont pourtant très concrètes : si à la suite d'une attaque vos données disparaissent et votre informatique s'arrête, êtes-vous prêts à retourner au papier et au crayon ?

Sans compter que les structures de taille petite, moyenne et intermédiaire sont particulièrement à risque : en l'absence de dispositifs de protection, elles sont une cible de choix pour les acteurs malveillants qui optimisent leurs gains en attaquant les plus vulnérables. Et si les entreprises les mieux préparées peuvent se remettre d'une attaque informatique, d'autres en sont durablement affectées.

Heureusement, nous pouvons aussi regarder le sujet de façon plus positive. Voire, faire de la « cyber » une opportunité ! Car en se protégeant –et, par capillarité, en protégeant leurs partenaires– les entreprises assurent leur pérennité et renforcent la confiance qui les lie à leurs parties prenantes. La cybersécurité représente donc un enjeu collectif majeur. Plus largement, elle est une clé essentielle pour le développement économique durable de la Nation.

Il y a une autre bonne nouvelle toutefois : l'application de quelques

bonnes pratiques permet déjà de réduire très significativement le risque. En mettant en place quelques mesures simples mais essentielles, vous pourrez protéger votre entreprise contre de nombreuses cybermenaces et considérablement limiter les dégâts en cas d'attaque de haut niveau. Il n'y a pas de solution miracle ou de risque zéro mais chaque organisation peut faire beaucoup pour sa propre sécurité !

Ce guide présente, en douze questions, des mesures accessibles pour une protection globale de l'entreprise. À vous de vous en emparer pour protéger votre activité et vos emplois. Certaines recommandations relèvent des bonnes pratiques, d'autres requièrent un investissement plus important pour lequel votre structure pourra être accompagnée. Elles vous permettront d'accroître votre niveau de sécurisation et de sensibiliser vos équipes aux bons gestes à adopter.

En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard. N'attendons pas que le pire arrive. Protégeons-nous !

Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

Thomas Courbe, directeur général des entreprises (DGE)

Avec le soutien de Cybermalveillance.gouv.fr

QUESTION N°1

CONNAISSEZ-VOUS BIEN VOTRE PARC INFORMATIQUE ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

« Ai-je connaissance des systèmes d'informations, applications et données vitales pour mon entreprise au regard de mon activité ? » : cette question est la toute première à se poser pour renforcer le système d'information de son entreprise. P**our bien se protéger, toute entreprise même unipersonnelle se doit d'inventorier ses matériels et logiciels ainsi que les données et les traitements qui constituent son patrimoine informationnel et contribuent à sa pérennité**. De cet inventaire découleront les mesures de protection adaptées.

Inventorier tous les équipements et les services

Ordinateur (et ses périphériques), mobile multifonction, tablette, serveur local, serveur distant (hébergement du site Web, service de messagerie, services logiciels en ligne, etc.). **Il faut aussi inventorier tous les périphériques : box, commutateurs, clés 4G, imprimantes etc**. Cet inventaire permet de savoir quoi protéger et d'identifier, dans une phase ultérieure, les biens critiques pour l'activité de l'entité.

Inventorier les logiciels utilisés

Il faut connaître leur nature, leurs fonctions principales et leurs versions. Il faut également s'assurer d'être en possession de licences d'utilisation valides, qui sont indispensables aussi bien du point de vue des obligations légales, que pour la maintenance.

Inventorier les données et les traitements de données

Quelles sont les données susceptibles d'affecter ou d'interrompre l'activité en cas de perte ou d'altération ? Quelles sont les données soumises à des obligations légales ? Y a-t-il un fichier client ? Où sont conservées les données, par exemple la comptabilité ? La même question se pose pour les traitements : quels sont les traitements dont l'altération affecterait ou interromprait particulièrement l'activité ?

Inventorier tous les accès

Il s'agit ici de déterminer qui se connecte au système d'information et quelles sont les modalités de chaque accès : catégorie de l'accédant (administrateur, utilisateur, invité), moyen d'accès (connexion locale ou distante), etc. Cet inventaire permettra de vérifier qu'aucun accès indu n'est maintenu (ancien employé, ancien prestataire) et ainsi de limiter la surface d'exposition aux menaces.

Inventorier les interconnexions avec l'extérieur

Quels sont les points de contact entre le système d'information de l'entreprise et Internet ? **Tout accès Internet, vers un prestataire ou un partenaire doit être recensé pour figurer ensuite dans l'inventaire**. Des règles de filtrage et de surveillance adaptées pourront y être associées.

Ce bilan indispensable permet de faire le point sur les besoins et les capacités numériques de son entreprise ; il doit être mis à jour régulièrement (au moins deux fois par an). Il permet également d'aider au choix des solutions numériques adaptées à l'entreprise, d'identifier les éventuels points de sécurisation à envisager, et, le cas échéant, de fournir un état des lieux détaillé qui aidera le prestataire sollicité pour cette tâche. Il sera aussi très utile pour les professionnels qui interviendront en réponse à incident en cas de compromission réelle.

POUR EN SAVOIR PLUS :

www.ssi.gouv.fr/guide/cartographie-du-systeme-dinformation

QUESTION N°2

EFFECTUEZ-VOUS DES SAUVEGARDES RÉGULIÈRES ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

Effectuer des sauvegardes régulières permet une restauration plus rapide des activités opérationnelles en cas d'incident, notamment en cas d'attaque par rançongiciel.

Identifiez les données à sauvegarder

Pour identifier les données, vous devez avoir inventorié préalablement tous vos matériels, puis déterminer quelles données sont essentielles à la poursuite de votre activité. Il peut s'agir de « données métier » (fichiers client, savoir-faire de fabrication par exemple), mais peut-être également des données techniques. Ces dernières, peuvent concerner la configuration des ordinateurs ou de tout ou partie de l'infrastructure de l'entreprise, notamment pour les outils de production industrielle.

Déterminez le rythme de vos sauvegardes

La fréquence des sauvegardes est à définir en lien avec le volume de données numériques produites sur un temps donné. Par exemple, une TPE/PME dans le secteur de l'artisanat pourra choisir une fréquence mensuelle de sauvegarde de ses factures et de son fichier client. En revanche, une TPE/PME de services pour qui les échanges dématérialisés constituent la valeur marchande pourra choisir une fréquence accrue, avec des sauvegardes hebdomadaires voire quotidiennes. Une sauvegarde différentielle peut être mise en place afin de retrouver différents points de sauvegarde : chaque jour ou chaque semaine pour les données métier, et chaque mois pour les données techniques.

Choisissez le ou les supports à privilégier pour votre sauvegarde

Il peut s'agir d'un support physique comme un disque dur externe, à déconnecter impérativement du système d'information à l'issue de la sauvegarde ou d'une sauvegarde dans un service nuagique (service commercialisé sous le terme *cloud*), voire des deux pour vos données les plus précieuses. Le support physique présente l'avantage d'être à l'abri d'une intrusion informatique, mais n'est pas à l'abri d'un vol, d'une destruction ou d'un dysfonctionnement. Les services nuagiques proposés aussi bien par les fournisseurs d'accès que par les éditeurs peuvent permettre une automatisation simple des sauvegardes mais sont plus exposés aux risques d'intrusion ou de panne. **Quelle que soit votre préférence de support, toute sauvegarde, une fois effectuée, doit faire l'objet d'un test pour vérifier son intégrité et sa viabilité lors d'une restauration**.

Évaluez la pertinence du chiffrement des données

Le chiffrement des données avant leur sauvegarde est une pratique recommandée. Elle concerne en priorité le stockage dans un service nuagique : en cas d'accès illégitime au service nuagique, les données restent protégées. Le choix de l'opérateur nuagique, les modalités de stockage des données et les conditions d'accès et d'authentification seront autant de points de vigilance à vérifier.

Respectez le cadre juridique

Les données dites « personnelles », qu'elles soient relatives aux employés ou à la clientèle, nécessitent des mesures de protection renforcées pour garantir leur intégrité, leur confidentialité, leur disponibilité et leur résilience en application du règlement général sur la protection des données (RGPD). **Les dispositifs juridiques de protection et de conservation des données s'appliquent quels que soient les objectifs du stockage (traitement ou sauvegarde)**. Qu'il s'agisse des obligations fiscales ou de protection des données personnelles, appliquez les mêmes mesures à vos sauvegardes qu'à votre système d'information.

POUR EN SAVOIR PLUS :

- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/sauvegardes
- www.ssi.gouv.fr/administration/reglementation/rgpd-renforcer-la-securite-des-donnees-a-caractere-personnel
- www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident

QUESTION N°3

APPLIQUEZ-VOUS RÉGULIÈREMENT LES MISES À JOUR ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

La majorité des attaquants recourent à des vulnérabilités publiques et documentées pour prendre pied sur les systèmes d'information : ils comptent soit sur la négligence des utilisateurs pour commettre leur forfait soit sur l'exploitation d'une vulnérabilité d'un service exposé sur Internet (par exemple un pare-feu, messagerie, etc.).

Il est indispensable d'effectuer les mises à jour des systèmes d'exploitation et de tout logiciel dès la mise à disposition des correctifs de sécurité par leurs éditeurs.

Utilisez des solutions matérielles et logicielles maintenues

Par habitude, par négligence ou par souci d'économies, il peut sembler tentant de conserver un matériel ou un logiciel au-delà de son « cycle de vie », c'est-à-dire après la période pendant laquelle son fabricant ou son éditeur garantit son maintien en conditions de sécurité. Tout matériel ou logiciel qui ne peut plus être mis à jour doit être mis au rebut ou désinstallé.

Activez la mise à jour automatique des logiciels et des matériels

Les mises à jour du système d'exploitation et de tous les logiciels utilisés doivent être effectuées dès que possible, à chaque mise à disposition d'un correctif par leurs éditeurs. Cela est d'autant plus important pour tous les matériels exposés sur Internet.

Il est recommandé d'activer les fonctions de mise à jour automatique proposées par les éditeurs.

Outre ces mises à jour régulières, des mises à jour hors calendrier

peuvent survenir en cas de détection d'une vulnérabilité dont la criticité ne permet pas d'attendre plusieurs semaines pour le déploiement d'un correctif. Ces mises à jour doivent aussi être appliquées dès que possible.

Si vous recourez à un sous-traitant

Assurez-vous qu'il effectue bien la mise à jour des systèmes numériques utilisés dans votre entreprise. Si nécessaire, exigez cette pratique dans vos contrats de sous-traitance.

POUR EN SAVOIR PLUS:

- www.ssi.gouv.fr/guide/guide-dhygiene-informatique
- www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques
- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mises-a-jour

QUESTION N°4

UTILISEZ-VOUS UN ANTIVIRUS ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE

Les antivirus sont très utiles à la protection des moyens informatiques : ils peuvent dans la majorité des cas empêcher une compromission et éviter une attaque par rançongiciel. **Un antivirus doit être déployé sur tous les équipements**, en priorité ceux connectés à Internet (postes de travail, serveurs de fichier, etc.). Un antivirus protège des menaces connues, qui évoluent très rapidement : des centaines de milliers de codes malveillants apparaissent chaque jour.

Il faut, pour cette raison, tenir à jour le logiciel en lui-même et sa base de données de signatures. Cette base de données est l'élément qui permet l'identification de programmes et fichiers malveillants : sans sa mise à jour fréquente, la protection offerte par l'antivirus s'en trouve très rapidement plus restreinte.

Les antivirus commerciaux proposent **une mise à jour automatique**, et un scan automatique des espaces de stockage : il est indispensable de procéder à l'activation de ces mécanismes dans les paramètres.

Par ailleurs, lors de l'achat d'un antivirus, il peut être intéressant, en fonction de vos usages, de souscrire aux fonctionnalités complémentaires proposées par de nombreux éditeurs logiciels tels qu'un pare-feu, un filtrage Web, un VPN, des outils anti-hameçonnage et de renforcement de la sécurité des transactions bancaires.

QUESTION N°5

AVEZ-VOUS IMPLÉMENTÉ UNE POLITIQUE D'USAGE DE MOTS DE PASSE ROBUSTES ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

Pourquoi choisir des mots de passe robustes ?

De nombreuses attaques sur Internet sont facilitées par l'utilisation de mots de passe trop simples ou réutilisés d'un service à l'autre. Les attaques contre des mots de passe peuvent être de différentes natures : attaques par force brute (l'attaquant tente le plus grand nombre de combinaisons possibles) ou par dictionnaires (l'attaquant tente les mots de passe les plus courants, qu'il s'agisse de noms communs ou de combinaisons simplistes comme « azerty »). Les attaques peuvent aussi être de type « ingénierie sociale » : l'attaquant teste alors des informations personnelles telles que les prénoms de vos proches ou les surnoms de vos animaux de compagnie après les avoir récupérés sur les réseaux sociaux. Enfin, ces attaques peuvent être effectuées à partir d'éléments déjà disponibles en ligne, parfois à votre insu, tels qu'une base de données mal sécurisée d'un fournisseur où figureraient vos identifiants pour un service donné.

Il faut ajouter qu'une attaque contre les mots de passe peut ne pas avoir comme finalité de se limiter au service impacté, mais permettre une propagation de l'attaque au sein de l'entreprise ou à ses partenaires. Par exemple, votre courriel pourrait être utilisé par l'attaquant pour adresser des courriels malveillants vers vos contacts professionnels afin de les inciter à faire des actions dangereuses à leur insu (comme cliquer sur un lien vers un site Internet compromis). Cette technique d'attaque pour le nom de hameçonnage (ou *phishing* en anglais). ▶

Qu'est-ce qu'un mot de passe robuste ?

- **L'ANSSI recommande que la longueur d'un mot de passe soit corrélée avec la criticité du service auquel il donne accès**, avec un minimum de **9 caractères pour les services peu critiques** (dont la compromission ne donnerait accès à aucune information personnelle, financière et n'impacterait pas le fonctionnement de l'entreprise) et un minimum de **14 caractères pour les services critiques** ;
- Un mot de passe robuste comporte **des capitales et des minuscules, des chiffres et des caractères spéciaux** ;
- Ces mots de passe ne doivent comporter aucun élément personnel (tel qu'une date de naissance ou un prénom);
- Il est possible d'avoir recours à une phrase de passe (*passphrase* en anglais). Les phrases de passe consistent à choisir aléatoirement un certain nombre de mots parmi un corpus déterminé (comme le dictionnaire de la langue française). Les *passphrases* sont souvent bien plus longues que les mots de passe « classiques », mais sont aussi pour certains utilisateurs plus simples à mémoriser.

Qu'est-ce qu'une bonne politique de mots de passe ?

- **Il faut des mots de passe différents pour chaque service nécessitant une authentification**. Il convient en particulier de ne jamais utiliser un même mot de passe pour sa messagerie personnelle et sa messagerie professionnelle ;
- Un coffre-fort de mots de passe peut vous aider à générer des mots de passe robustes et ne pas avoir à les mémoriser. Il permet de sauvegarder l'ensemble des mots de passe dans un fichier chiffré, accessible uniquement par un seul et unique mot de passe. Il est préférable d'utiliser un coffre-fort certifié par l'ANSSI ;
- Le succès d'une bonne politique de choix des mots de passe nécessite une sensibilisation des utilisateurs aux risques liés au choix d'un mot de passe qui serait trop facile à deviner.
  Il faut activer une authentification multifacteurs quand elle est proposée par le fournisseur de service (mail, banque, etc.). De nombreux services permettent désormais de renforcer le

mot de passe par une authentification secondaire : en plus du mot de passe, la saisie d'un second élément est nécessaire. Il est recommandé d'activer ce paramètre dès qu'il vous est proposé.

POUR LES PME

Il convient idéalement d'implémenter une authentification multi-facteurs par jeton physique (carte à puce, token USB, etc.) pour simplifier l'accès aux terminaux de l'entreprise.

Pour les PME qui disposent de nombreuses solutions logicielles centralisées (messagerie, services Web internes, etc.), l'activation d'un service d'authentification unifié (type *single sign on*) permet de simplifier et de renforcer les mécanismes d'authentification.

Pour encadrer et vérifier l'application de ces règles, une PME pourra recourir à des mesures parmi lesquelles :

- le blocage des comptes à l'issue de plusieurs échecs de connexion, ce blocage pouvant être temporaire ou permanent ;
- la désactivation des options de connexion anonyme (comptes « invité ») ;
- la mise en place d'une politique robuste des mots de passe sur les serveurs d'authentification.

POUR EN SAVOIR PLUS :

- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/mots-de-passe
- www.ssi.gouv.fr/guide/mot-de-passe

QUESTION N°6

AVEZ-VOUS ACTIVÉ UN PARE-FEU ? EN CONNAISSEZ-VOUS LES RÈGLES DE FILTRAGE ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À EXPERT

Pourquoi activer le pare-feu local ?

Ce logiciel, installé sur l'ordinateur de l'utilisateur, protège principalement contre des attaques provenant d'Internet. Pour les entreprises disposant d'un système d'information d'entreprise, il permet également de ralentir ou limiter l'action d'un acteur malveillant ayant réussi à prendre le contrôle d'un des postes de travail. Les attaquants tentent souvent d'étendre leur intrusion aux autres postes de travail pour prendre entièrement le contrôle du système et, *in fine*, accéder aux documents des utilisateurs. L'activation du pare-feu rend plus difficile ce déplacement latéral.

Comment procéder ?

POUR LES TPE

Sans connaissance informatique particulière, l'activation d'un pare-feu préinstallé sur le poste de travail et son paramétrage par défaut (qui bloque toute connexion entrante), constituent un premier niveau de protection. Un pare-feu local est une fonction disponible sur la plupart des systèmes d'exploitation grand public. Des pare-feux sont également commercialisés en complément de suites logicielles antivirales.

POUR LES PME

Un pare-feu local (qu'il soit intégré au système d'exploitation ou qu'il soit une solution logicielle tierce), doit être installé sur tous

les postes de travail. Il est recommandé d'assurer l'homogénéité des configurations et de la politique de filtrage des flux.

Une politique de filtrage minimale :

- bloque tous les flux non strictement nécessaires (en particulier les connexions entrantes depuis Internet) ;
- journalise les flux bloqués.

Par ailleurs, une PME doit déployer des pare-feux physiques en priorité pour protéger l'interconnexion du SI à Internet, voire, pour les entités les plus matures en matière de sécurité ou disposant d'une masse critique, pour segmenter le réseau interne en zones ayant des niveaux différents de sensibilité et d'exposition aux menaces (zone des postes de travail utilisateurs, zone des serveurs internes, zone des serveurs exposés sur Internet, zone des systèmes industriel et outils de production, etc.).

S'agissant de l'interconnexion à Internet, elle se traduira idéalement par la mise en œuvre d'une zone « démilitarisée » (DMZ), constituée de pare-feux mais aussi de services de rebond, principalement pour la messagerie et la navigation Web.

Pour une configuration adaptée à vos usages, n'hésitez pas à recourir aux services d'un prestataire informatique labellisé ExpertCyber. Une mise en relation est proposée par le site Cybermalveillance.gouv.fr.

POUR EN SAVOIR PLUS :
Mise en œuvre de pare-feux physiques : www.ssi.gouv.fr/uploads/2018/01/guide_preconisations-pare-feux-zone-exposee-internet_anssi_pa_044_v1.pdf

QUESTION N°7

COMMENT SÉCURISEZ-VOUS VOTRE MESSAGERIE ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE *(TPE)* **/ MOYENNE À EXPERT** *(PME)*

POUR LES TPE

La messagerie est le principal vecteur d'infection du poste de travail, qu'il s'agisse de l'ouverture de pièces jointes contenant un code malveillant ou du clic malencontreux sur un lien redirigeant vers un site lui-même malveillant (*phishing* ou hameçonnage).

Quelques réflexes permettent de se prémunir des tentatives de hameçonnage : l'expéditeur est-il connu ? Une information de sa part est-elle attendue ? Le lien proposé est-il cohérent avec le sujet évoqué ? En cas de doute, une vérification de l'authenticité du message par un autre canal (téléphone, SMS, etc.) auprès de l'émetteur est nécessaire.

Par ailleurs, la redirection de messages professionnels vers une messagerie personnelle est à proscrire car cela constitue un vecteur de fuite irrémédiable d'informations de l'entité.

POUR LES PME

Que l'entité héberge ou fasse héberger son système de messagerie, elle doit s'assurer :

- de disposer d'un système d'analyse antivirus en amont des boîtes aux lettres des utilisateurs pour prévenir la réception de fichiers infectés ;
- de l'activation du chiffrement TLS des échanges entre serveurs de messagerie (de l'entité ou publics) ainsi qu'entre les postes utilisateur et les serveurs hébergeant les boîtes de messagerie électronique.

Pour se prémunir d'escroqueries connues (ex : demande de virement frauduleux émanant vraisemblablement d'un dirigeant), des mesures organisationnelles doivent être appliquées strictement.

Il est souhaitable de ne pas exposer directement les serveurs de messagerie électronique d'entreprise sur Internet. Dans ce cas, un serveur relai dédié à l'envoi et à la réception des messages doit être mis en place en coupure d'Internet.

POUR EN SAVOIR PLUS :

- www.ssi.gouv.fr/entreprise/precautions-elementaires/5-reflexes-a-avoir-lors-de-la-reception-dun-courriel
- www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing
- www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-tls

QUESTION N°8

COMMENT SÉPAREZ-VOUS VOS USAGES INFORMATIQUES ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

L'interconnexion des outils informatiques avec Internet présente un certain nombre de risques, parmi lesquels on peut citer :

- l'exfiltration de données depuis l'entreprise vers Internet, portant ainsi atteinte à leur confidentialité voire à la réputation de l'entreprise si elles sont diffusées ;
- l'intrusion depuis Internet pour porter atteinte à l'intégrité ou la disponibilité du SI et des outils de production de l'entreprise ;
- l'usurpation d'identité ;
- le détournement du SI de l'entreprise pour des usages frauduleux ou délictueux.

Comment diminuer l'exposition à ces menaces ?

Le premier principe d'hygiène repose sur la création de comptes utilisateurs dédiés à chaque employé et ne disposant pas de privilège d'administration. Ceci permet de limiter le risque d'installation de code malveillants.

Seuls les comptes utilisateur doivent être utilisés pour la navigation sur Internet : en effet, de très nombreuses attaques sont causées par une navigation effectuée depuis un compte doté de privilèges administrateur, ce qui facilite grandement la tâche d'un attaquant pour prendre le contrôle complet de l'ordinateur. Les comptes d'administration doivent être utilisés uniquement pour configurer les équipements ou installer des logiciels. **Les comptes et leurs privilèges doivent être tenus à jour : quand un collaborateur quitte l'entreprise, il convient de faire l'inventaire**

de ses accès et de tous les révoquer, de telle sorte que lui-même ou un tiers ne puisse plus y accéder.

Par ailleurs, l'idéal est de posséder un ordinateur uniquement dédié à sa pratique professionnelle, sans usage personnel et familial. Cependant en cas d'usages multiples sur une seule et même machine, il est alors recommandé de créer des comptes utilisateur pour chaque usage.

Ces cloisonnements d'usage sont faciles à implémenter même par un entrepreneur individuel, sur sa propre machine. Ils permettent de contrer l'exécution arbitraire d'un certain nombre de programmes malveillants.

Depuis un mobile multifonctions ou une tablette, les tâches d'administration et de cloisonnement s'effectuent d'une autre manière : **il faut limiter les autorisations données à chaque application pour chacune de leurs utilisations et télécharger les applications uniquement depuis les marchés officiels** ou le site Internet des éditeurs.

POUR LES PME

Les PME qui comportent un plus grand nombre de collaborateurs et un réseau informatique de plusieurs machines prendront également avantage à respecter les mesures suivantes, ou les faire appliquer par leur prestataire :

- Les connexions entre les postes des utilisateurs doivent être interdites par défaut : si un poste est infecté par un code malveillant, ce cloisonnement évite la propagation directe sur l'ensemble des autres postes ;
- En matière d'administration du SI de l'entreprise, les postes et les comptes d'administration doivent être dédiés à cet usage ;
- Si les ressources de l'entreprise s'y prêtent, les activités numériques de l'entreprise doivent être cloisonnées en différentes zones réseaux par des dispositifs de filtrage physiques ou virtualisés (zone des serveurs internes, zone des serveurs exposés sur Internet, zone des postes de travail utilisateurs, zone d'administration, zone système industriel, etc.). Il est recommandé de vous faire accompagner par des professionnels de l'informatique pour bénéficier de l'architecture sécurisée adaptée à votre système d'information et à la nature de vos données.

POUR EN SAVOIR PLUS :

- www.ssi.gouv.fr/guide/definition-dune-architecture-de-passerelle-dinter-connexion-securisee
- www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/securite-usages-pro-perso

QUESTION N°9

MAÎTRISEZ-VOUS LE RISQUE NUMÉRIQUE LORS DES MISSIONS ET DES DÉPLACEMENTS PROFESSIONNELS ?

PUBLIC : TOUS
DIFFICULTÉ : FACILE

L'emploi d'ordinateurs portables, de mobiles multifonctions ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Le renforcement contraint au télétravail a également augmenté le recours à des solutions de mobilité.

Tout en facilitant la continuité d'activité, ces usages présentent des risques spécifiques.

Que prévoir avant de partir en mission ?

- sauvegardez vos données pour les retrouver en cas de perte ou de vol des équipements ;
- équipez vos équipements d'écrans de confidentialité ;
- vérifiez que vos mots de passe ne sont pas préenregistrés ;
- dans la mesure du possible, procéder au chiffrement de vos données les plus sensibles ou de l'ensemble du disque dur.

Quels réflexes pendant la mission ?

- gardez vos appareils, supports et fichiers avec vous ;
- informez votre entreprise en cas de perte ou de vol de votre matériel ;
- refusez la connexion d'équipements appartenant à des tiers à vos propres équipements (ordiphone, clé USB, baladeur, etc.).

Après la mission

- n'utilisez jamais les clés USB qui peuvent vous avoir été offertes lors de vos déplacements (salons, réunions, etc.) : très prisées des attaquants, elles sont susceptibles de contenir des programmes malveillants.

POUR LES PME

Prévoir le cas des voyages en dehors de l'UE et les recommandations suivantes :

Avant :

- n'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission et ne contenant que les données nécessaires ;
- apposez un signe distinctif sur vos appareils pour vous assurer qu'il n'y a pas d'échange pendant le transport ;
- dans le cas où vous devez accéder à distance aux systèmes d'information de l'entreprise, prévoyez l'installation d'un logiciel de connexion à distance de type VPN (*virtual private network*) afin de protéger vos communications.

Pendant :

- gardez vos appareils, supports et fichiers avec vous pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un coffre d'hôtel) ;
- retirez la carte SIM si vous êtes contraint de vous séparer de votre téléphone ;
- informez votre entreprise en cas de perte ou de vol d'inspection ou de saisie de votre matériel par des autorités étrangères ;
- n'utilisez pas les équipements que l'on vous offre ;
- ne connectez pas vos équipements à des postes qui ne sont pas de confiance. Si vous avez besoin d'échanger des documents lors d'une présentation commerciale, préférez les échanges par mail ou utilisez une clé USB destinée uniquement à cet usage et effacez ensuite les données avec un logiciel d'effacement sécurisé. Si vous devez recharger votre mobile, ne le connectez pas à un ordinateur non maîtrisé ou à une prise USB en libre-service dans les aéroports.

Après :

- effacez l'historique des appels et de navigation ;
- changez les mots de passe que vous avez utilisés pendant le voyage ;
- faites analyser vos équipements après la mission, si vous le pouvez.

POUR EN SAVOIR PLUS :
www.ssi.gouv.fr/guide/partir-en-mission-avec-son-telephone-sa-tablette-ou-son-ordinateur-portable

QUESTION N°10

COMMENT VOUS INFORMEZ-VOUS ? COMMENT SENSIBILISEZ-VOUS VOS COLLABORATEURS?

PUBLIC : TOUS
DIFFICULTÉ : FACILE À MOYENNE

POUR LES TPE : S'INFORMER

Sans avoir de compétences particulières en informatique ni beaucoup de temps à y consacrer, il est possible de prendre connaissance de recommandations concernant les bonnes pratiques, d'alertes sur les menaces en cours et d'informations sur les mises à jour logicielles disponibles en suivant les actualités publiées par le dispositif Cybermalveillance.gouv.fr. Ce suivi ne nécessite aucune compétence informatique particulière.

POUR LES PME : S'INFORMER ET SENSIBILISER

Pour aller plus loin, une veille technique relative aux campagnes d'attaques et aux vulnérabilités est également effectuée par le centre gouvernemental de veille, d'alertes et de réponse aux attaques informatiques, le CERT-FR. Elle conviendra plus particulièrement aux PME dotées d'un service informatique, mais aussi aux professionnels indépendants qui souhaitent élargir leurs connaissances.

Au-delà, pour les PME, il est recommandé de mettre en place les bases d'une culture de l'hygiène informatique par une information régulière du personnel aux bonnes pratiques de sécurité et aux principales menaces qui peuvent affecter la vie de l'entreprise. Cette sensibilisation peut se décliner par le biais d'une charte informatique remise à chaque nouvel arrivant, qui détaille les usages numériques à respecter et la procédure de

déclaration d'un incident. Elle se doit d'être régulièrement rappelée : il peut s'agir, par exemple, de diffusions régulières de messages en interne, lors de réunions ou par le biais d'une newsletter éventuellement étayée par une revue de presse des incidents récents.

La déclaration d'incidents doit être encouragée et, pour ce faire, une réponse non coercitive doit être privilégiée. Il s'agit de responsabiliser les utilisateurs face à des menaces évolutives et non de les sanctionner (sauf en cas d'action délibérée) afin d'éviter une sous-déclaration des incidents.

POUR EN SAVOIR PLUS :

- www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-proteger-vos-donnees-en-sensibilisant-vos-collaborateurs
- cert.ssi.gouv.fr

QUESTION N°11

AVEZ-VOUS FAIT ÉVALUER LA COUVERTURE DE VOTRE POLICE D'ASSURANCE AU RISQUE CYBER ?

PUBLIC : PME
DIFFICULTÉ : MOYENNE

Les sociétés d'assurance proposent de plus en plus des clauses permettant de se prémunir de certains risques d'origine numérique afin d'accompagner les entreprises victimes de cybermalveillance ou de cyberattaques. L'assurance fournit, en cas de sinistre, une assistance juridique ainsi qu'une couverture financière du préjudice (matériel, immatériel, etc.).

Selon les contrats, différents types de protection peuvent être proposés : usurpation d'identité, garanties contre une perte d'exploitation, accompagnement juridique pour une déclaration d'atteinte aux données personnelles, prise en charge d'un accompagnement technique pour la restauration du système d'information après une cyberattaque.

Ces clauses assurantielles peuvent se traduire dans les contrats d'assurance classique ou prendre la forme d'une police d'assurance « cyber » spécifique, bien que ce dernier marché reste encore à développer, en particulier en matière de jurisprudence concernant l'activation ou non des clauses d'exclusion.

Sous quelque forme que ce soit, il est important de vérifier que les risques les plus redoutés pour la pérennité de l'entreprise sont couverts.

POUR EN SAVOIR PLUS :
www.cybermalveillance.gouv.fr/tous-nos-contenus/la-federation-francaise-de-lassurance

QUESTION N°12

SAVEZ-VOUS COMMENT RÉAGIR EN CAS DE CYBERATTAQUE ?

PUBLIC : PME
DIFFICULTÉ : MOYENNE À EXPERTE

Préparez-vous à l'incident

Les TPE et PME ont tout avantage à identifier préalablement des prestataires spécialisés dans la réponse aux incidents de sécurité.

Pour les TPE et les PME (mais aussi les particuliers et les collectivités), le gouvernement a mis en place la plateforme Cybermalveillance.gouv.fr. Après avoir réalisé un diagnostic en ligne, les victimes accèdent à des conseils personnalisés leur permettant de résoudre leur problème. Elles peuvent également être mises en relation avec des professionnels de proximité pour les assister. Il ne faut pas non plus hésiter à vous rapprocher de votre chambre des métiers (CMA) ou de votre chambre du commerce (CCI) : leurs experts peuvent vous orienter vers une assistance appropriée.

En cas d'incident avéré

Le premier réflexe à avoir en cas d'incident concernant un système d'information est de déconnecter son équipement ou son SI d'entreprise d'Internet. Pour un équipement individuel, cela peut se traduire par le retrait de la prise ou la désactivation des services WiFi. Pour un SI d'entreprise, l'action peut être menée sur l'équipement réseau ou le pare-feu d'entreprise. Cela empêchera l'attaquant de piloter son attaque telle qu'un rançongiciel, et cela évitera une exfiltration éventuelle de données.

N'éteignez pas ni ne modifiez les ordinateurs et matériels affectés par l'attaque : ils seront utiles aux enquêteurs.

En cas de rançongiciel, ne payez jamais la rançon demandée : des solutions de déchiffrement existent : vous serez assisté par les gardiens de la paix. Vos ▶

sauvegardes vous permettront de retrouver une activité normale (cf. Question n°2).

Il est recommandé d'ouvrir une main courante pour tracer les actions et les événements liés à l'incident. Chaque entrée de ce document doit contenir, a minima :

- l'heure et la date de l'action ou de l'événement ;
- le nom de la personne à l'origine de cette action ou ayant informé sur l'événement ;
- la description de l'action ou de l'événement.

La tenue d'une main courante régulièrement alimentée tout au long de l'incident va considérablement faciliter l'intervention du prestataire et la résolution du problème.

Pour une PME, il convient de concevoir et de déployer un dispositif de communication (messages, communication interne, communication partenariale, réseaux sociaux, relations presse, etc.). Ce dispositif doit être proposé par le service communication (en lien avec les experts techniques) et porté par les dirigeants de l'entreprise.

La charte informatique peut également informer les collaborateurs de la bonne attitude à avoir en cas d'incident avéré.

Aspects juridiques

Les entreprises traitant des informations personnelles, relevant du Règlement général sur la protection des données personnelles (RGPD) sont soumises au respect des exigences de ce texte. En cas d'incident, elles sont également tenues d'informer la CNIL et leurs clients.

Il est essentiel de porter plainte. Vos matériels affectés et vos journaux seront très utiles aux enquêteurs. En cas de demande de rançon, ne pas la payer.

En cas de fuites de données personnelles, il est obligatoire de faire une déclaration auprès de la CNIL.

POUR EN SAVOIR PLUS :

- www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident
- www-org.gendarmerie.interieur.gouv.fr/nos-conseils/pour-les-professionnels/cybermenaces-comment-proteger-votre-entreprise
- www.cybermalveillance.gouv.fr/cybermenaces
- www.gouvernement.fr/risques/cybercriminalite
- www.cnil.fr/fr/notifier-une-violation-de-donnees

Ce guide présente, en douze questions, des mesures accessibles pour une protection globale de l'entreprise. Certaines recommandations relèvent des bonnes pratiques, d'autres requièrent un investissement plus important pour lequel votre structure pourra être accompagnée. Elles vous permettront d'accroître votre niveau de sécurisation et de sensibiliser vos équipes aux bons gestes à adopter. À vous de vous en emparer pour protéger votre activité et vos emplois.

En l'absence de préparation, lorsque l'incident survient, il est déjà trop tard. N'attendons pas que le pire arrive. Protégeons-nous !

Version 1.0 – Février 2021 – **ANSSI-GP-086**
Dépot légal : février 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI — 51, boulevard de la Tour-Maubourg — 75 700 PARIS 07 SP
www.ssi.gouv.fr — communication@ssi.gouv.fr