Courriels

Poste informatique

Les règles de la sécurité informatique

Usages de base pour la sécurisation des équipements numériques

Wifi

Firewall

Sécurité

Mots de passe

Sauvegarde

WWW

AEIM

ZA Jeanberty
47350 SEYCHES

Tel : 05 53 83 47 50

Révision 2.02 – 03/2016

Traces

Emmanuel ANDRÉ
Gérant de AEIM – 47350 Seyches
Président de la Fédération des Revendeurs et Prestataires Informatiques

« La sécurité informatique est un défi quotidien. Cybercriminalité est désormais un terme entendu chaque jour. Derrière un acte de cybercriminalité, l'auteur peut aussi bien être un amateur éclairé qu'une véritable bande organisée, qui attaque tout type de cibles et particulièrement les PME, TPE, qui sont encore peu ou pas sensibilisées à ce phénomène de malveillance, lequel se présente sous différentes formes : cela peut aller du simple exploit d'intrusion à la destruction totale des données. Entre les deux, l'espionnage (tant économique qu'industriel), la fraude aux moyens de paiements, l'usurpation d'identité pour récupérer des informations et plus récemment, le cryptage complet des données avec demande de rançon à la clé.

Parce que notre quotidien a profondément été bouleversé avec l'ère numérique (les courriels ont remplacé les courriers, les sites internet ont supplantés les catalogues, les services bancaires sont devenus « en ligne », les documents commerciaux (devis, bons de commande, bons de livraison, factures) sont devenus des éléments dématérialisés et parce que d'une manière générale, le document numérique a pris le pas sur le document traditionnel, de nouvelles menaces sont nées de ce bouleversement. Et nous ne sommes qu'au tout début de l'ère numérique.

Si aucune solution n'est durable face aux menaces et à la complexité et l'ingéniosité des outils et des astuces mis en œuvre par les cybercriminels, ce guide a pour vocation de présenter les règles de bases de la sécurité. La base de la sécurité doit être une prise de conscience de l'existence des risques. Il faut ensuite garder à l'esprit qu'il n'existe pas de solutions miracle pour ne pas être soumis à ces risques : il faut donc être sensibilisé aux risques, et adopter les bonnes pratiques pour tenter de minimiser l'impact de ces risques.

Les informations et recommandations présentées dans ce guide dévoilent un aperçu des usages préconisés en termes de sécurité informatique. »

TABLE DES MATIERES

1 – La sécurisation physique des lieux de stockage de données

- Sécuriser un système informatique ne sert à rien si ce dernier est facilement accessible ! Le vol physique de postes de travail, ou pire de serveurs, permet, une fois le matériel récupéré, de prendre tout son temps pour analyser et passer outre les sécurités mises en place.

C'est la première règle : faire en sorte que les systèmes informatiques ne puissent pas être dérobés.

Les lieux doivent donc être protégés, difficiles d'accès une fois l'établissement fermé au public. La mise en place de systèmes de fermetures avec des serrures difficilement fracturables, la sécurisation des locaux par systèmes d'alarme de détection de présence, détection d'ouverture sont nécessaires.

Au-delà de ces préventions contre l'accès, les systèmes de déclenchement de brouillard s'avèrent très efficaces.

Les systèmes de vidéo surveillance avec alerte en temps réel sur smartphone sont également des solutions permettant de prévenir une intrusion en cours dans le pire des cas, une intrusion allant se produire dans le meilleur des cas.

Pour les serveurs de données ou d'applications ainsi que pour les serveurs NAS faisant office de sauvegarde centralisée, il est nécessaire de sur-sécuriser le local hébergeant ces systèmes, afin de retarder ou d'empêcher l'accès à ces éléments critiques.

2 – La sécurisation des accès au réseau interne

- Laisser un tiers (représentant, commercial, client, fournisseur…) se connecter à votre réseau internet est devenu une pratique courante. En se connectant à votre réseau internet, il se connecte aussi à votre réseau informatique.

Il est donc nécessaire de scinder réseau interne d'une part et accès externe d'autre part, afin de pouvoir continuer d'offrir la facilité de connexion à internet, tout en bloquant l'accès à vos postes informatiques. Pas nécessairement parce que le tiers qui s'y connecte aurait de mauvaises intentions. Ce n'est surement pas le cas. Mais parce qu'à son insu son poste informatique peut être porteur d'éléments malsains qui vont s'étendrent sur vos propres postes. Bloquer l'accès à votre réseau interne est donc une sécurité nécessaire.

Et ce tant pour les connexions wifi, que pour les connections filaires. Il est nécessaire de s'équiper de commutateurs réseaux, dits « Switchs », qui soient manageables, permettant ainsi de créer des réseaux virtuels (Vlan).

Avec de telles solutions matérielles, il est ainsi possible de dissocier les réseaux : en créant un réseau « invité », ou seul internet sera accessible depuis un point identifié. Tandis que sur votre réseau « privé », l'ensemble de vos postes communiquent entre eux, d'une part, avec internet d'autre part, sans être ni vus ni accessibles par le réseau « invité ».

Dans la mesure du possible, il est déconseillé d'activer un réseau Wifi en entreprise. Les données qui transitent en Wifi sont facilement récupérables et exploitables par un utilisateur averti ou mal intentionné. La connexion par câble ethernet, dite connexion filaire, est un choix qu'il faut privilégier. Jusqu'à peu, la connexion filaire bénéficiait de 2 avantages : sa sécurité renforcée par rapport au wifi, et sa vitesse de connexion.

Cependant, de nouveaux points d'accès Wifi arrivent sur le marché, avec des vitesses de connexions supérieures à celles des connexions filaires : 1,7 Giga pour les nouveaux équipements Wifi, contre 1 Giga pour les équipements filaires. Le gain de vitesse (annoncé sur le papier) par ces nouveaux équipements Wifi est finalement négligeable dans une utilisation quotidienne et de nouveaux réseaux filaires à 10 Giga sont de plus en plus couramment annoncés chez certains constructeurs. Pour l'instant, leur coût est prohibitif mais leur commercialisation en masse permettra une réduction importante des coûts à court terme.

Dans certains cas, (utilisation de portables, de tablettes), l'utilisation du Wifi est une obligation. Alors il est nécessaire de sécuriser l'accès par la création de Vlan (réseau virtuel), et également par une gestion très stricte des équipements connectés. Chaque équipement informatique possède une adresse réseau unique (adresse MAC). Les équipements Wifi professionnels permettent de n'autoriser que certaines adresses MAC à se connecter sur le réseau.

Les cybercriminels ont trouvé la parade avec la technique du « Mac Spoofing » (se faire passer pour un équipement reconnu et autorisé sur le réseau), mais la mise en œuvre est encore complexe et ne reste accessible qu'à certains.

Le choix d'une clé de sécurité complexe avec un chiffrement adapté (WPA Entreprise) est nécessaire.

Le point d'accès Wifi doit être en mesure d'enregistrer un journal de connexion, qui doit être régulièrement vérifié. Il doit également être en mesure de définir des plages horaires de connexions, permettant ainsi de stopper tout accès Wifi pendant les horaires de fermeture de l'établissement.

Enfin, si vous communiquez la clé d'accès wifi à des tiers pour qu'ils puissent se connecter temporairement, changez de clé régulièrement.

3 – La sauvegarde des données

- Je me plais souvent à annoncer : « J'ai 2 types de clients : ceux qui ont déjà perdu leurs données, et ceux qui vont les perdre. »

C'est une réalité : une règle importante à toujours avoir à l'esprit avec l'informatique, est de ne pas faire confiance à l'informatique !

Il existe de nombreux moyens d'assurer la sauvegarde des données. Tous ne sont pas fiables. Dans le cadre d'un usage professionnel, on oubliera rapidement les « clés Usb » et « disques externes », solutions plutôt dédiées à un usage privé, pour assurer la sauvegarde de 2 albums de musiques et 3 photos…

Les supports CD et DVD sont également à bannir, pour plusieurs raisons : les temps de sauvegarde sont excessivement longs, les supports sont de faibles capacités, et la fiabilité de ces supports dans le temps est médiocre.

La sauvegarde interne : Elle peut être réalisée sur un serveur NAS (boîtier dédié contenant 1 ou plusieurs disques durs de grande capacité).

Avantages : accessible par le réseau interne, le serveur NAS permet de réaliser une ou plusieurs sauvegardes par jour, (temps de sauvegarde assez rapide, en temps réel) sans impacter le fonctionnement des utilisateurs.
Inconvénient : Le serveur NAS reste dans les mêmes locaux que les postes informatiques et, en cas d'incendie, dégâts des eaux ou vol, la perte peut être totale.

La sauvegarde externe : plusieurs solutions peuvent être envisagées.

1/ Pour maitriser et conserver en interne l'intégralité des sauvegardes, un second serveur NAS peut être installé sur un site distant et à période définie (généralement à partir de la fin de la journée), le serveur NAS interne se réplique sur le serveur Nas Distant. Cette méthode est couramment utilisée, mais est

contraignante : elle impose un double investissement au niveau des serveurs NAS d'une part, une connexion internet de très grande qualité et très rapide d'autre part. Enfin, elle suppose que l'entreprise dispose d'au moins 2 sites, physiquement éloignés l'un de l'autre, bénéficiant chacun de connexions internet « robustes ».

2/ La sauvegarde « Dans le Cloud ».

Il est nécessaire de sélectionner un hébergeur agréé. Certains corps de métiers (santé, industries sensibles, collectivités, entreprises intervenant pour l'armée et l'industrie militaire) sont tenus à certaines obligations. Les pseudo-hébergeurs (fournisseurs d'accès, sites internet…) ne sont pas recommandés pour le peu de garanties de sécurité proposées, par le flou concernant la localisation des centres de sauvegardes et la faiblesse ou l'absence de chiffrement des données sauvegardées, ainsi que la confidentialité des données sauvegardées.

Il est donc nécessaire de se rapprocher d'un hébergeur fiable, proposant le cryptage des données sauvegardées dès leurs transmissions depuis le poste client.

D'autre part, certains hébergeurs professionnels proposent désormais une rétention des données sur plusieurs semaines, permettant jusqu'à 4 semaines de sauvegarde. En cas d'attaque par un virus de type crypto-locker (qui a pour but d'encoder les données clients pour les rendre inaccessibles), il est possible de récupérer les 28 derniers jours de sauvegarde, (permettant ainsi d'avoir une véritable solution de reprise d'activité), et non pas seulement la dernière sauvegarde réalisée, pour peu que celle-ci soit cryptée par le virus et devienne donc inexploitable.

Les hébergeurs professionnels réalisent eux-mêmes une sauvegarde de leur data-center sur un second site distant. Dans ces conditions, la sécurité des données est particulièrement fiable.

Fréquence : Une sauvegarde opérationnelle est une sauvegarde quotidienne, voire multi-quotidienne !

Vérification : La vérification régulière de l'intégrité des données sauvegardées est un impératif. Cette vérification permet de certifier que la restauration des données en cas d'incident est possible.

4 – Le choix des mots de passe

- La plupart des cas de piratage ou d'intrusion est lié à la facilité à découvrir un mot de passe trop simple, trop court, trop évident, trop « 1234 ».

1/ Ayez de la mémoire. Ne notez pas vos mots de passe. Ne faites pas un fichier « Excel » de vos mots de passe. Pire, ne sauvegardez pas ce fichier dans le « cloud ». Ne l'envoyez pas par mail sur votre messagerie personnelle ou sur la messagerie d'un collègue ! Oubliez le traditionnel papier collé sur l'écran avec les mots de passe inscrits, bien en évidence !

2/ Choisissez un mot de passe complexe si possible : 9, 12, 16 caractères. Il doit comprendre un mélange de lettres, de chiffres et de caractères spéciaux. Pour les lettres, utilisez des majuscules et des minuscules. Un mot de passe sécurisé pourrait ressembler à cela : Y6!tpM4Rsm$(2

Inconvénient : il n'est pas forcément simple à retenir. Une méthode permettant d'avoir un mot de passe complexe, mais facilement mémorisable est celle de la phrase. Imaginons que vous ayez 4 chats et 2 chiens. Exemple : « J'ai 4 chats : Horos, Gribouille, Toupie, Gandhi, et 2 chiens : Plouf et Zig-Zag ». Traduit en mot de passe, cela donne : J'a4c:HGTGe2c:PZ (La première lettre de chaque mot est récupérée pour générer le mot de passe).

3/ N'utilisez jamais un mot de passe basé sur un mot existant, comme un prénom, une ville, une date de naissance, votre nom à l'envers, le nom de votre animal de compagnie…

4/ Ayez toujours un mot de passe différent de celui de votre mot de passe de messagerie.

5/ Pour les sites ou applications sensibles, changez régulièrement de mot de passe : mensuellement ou au trimestre.

6/ Si un mot de passe vous est automatiquement généré, changez-le dès votre première connexion.

7/ Pour les appareils permettant les connexions à internet, les commutateurs réseaux manageables, les imprimantes : changez le mot de passe dès réception (admin dans 90 % des cas). Idem avec les appareils Bluetooth (0000).

8/ Ne mémorisez pas les mots de passe dans les navigateurs

9/ L'importance du mot de passe sur votre ordinateur est très relative, il faut moins d'une minute à une personne initiée pour le découvrir ou pour utiliser le poste sans avoir besoin du mot passe.

10/ Ayez des mots de passe différents selon les applications.

5 – Les courriels

- Au rythme de 30, 50, 100 courriels par jour, le risque d'infection ou d'attaque par ce biais est un des plus importants qui soit. Il suffit d'une erreur d'appréciation et d'un clic malheureux.

Si les courriels abolissent les délais de transmission d'informations, ils sont dans le même temps devenus encombrants, envahissants et dangereux.

Les dangers : les courriels comportant des pièces jointes infectées, les courriels mentionnant un lien vers un site internet, les courriels imitant un courriel qui pourrait être officiel, et enfin les courriels qui proviennent d'un de vos contacts, sans que ce contact ne vous ait rien expédié !

1 / Prenez le temps de lire. Vérifiez l'adéquation nom de l'expéditeur / adresse mail de l'expéditeur / contenu du mail.

2/ N'ouvrez pas de pièce jointe si vous ne connaissez pas l'expéditeur.

3/ Supprimez sans hésitations les courriels demandant des informations personnelles (mot de passe, coordonnées bancaires) ou vous invitant à cliquer sur un lien pour vous identifier sur un site. Il s'agit très souvent de Phishing (apparence d'une institution / entreprise), vous envoyant sur un site qui « ressemble » au site officiel, mais se trouve en réalité être un « faux site », dont le but est de récupérer vos identifiants de connexion.

4/ Ne faites pas suivre les courriels de type chaîne (appel à la générosité, grand malheur si non envoi du courriel à d'autre contacts, fausses alertes…).

5/ Jamais une institution ne vous enverra un courriel avec des fautes d'orthographes !

6/ Hélas non ! Vous n'avez pas gagné 20.000.000 Euros à la grande loterie organisée par Microsoft ou par un tirage au sort Européen en provenance du gouvernement Espagnol. Ne cliquez pas sur les offres irréelles non sollicitées par vos soins.

7/ Si un lien est présent dans le courriel et que le courriel vous semble officiel, le fait de positionner la souris sur le lien vous indique quel site va être ouvert dans le navigateur. Assurez-vous que le lien vers le site est celui que vous utilisez habituellement. Préférez plutôt le lancement de votre navigateur et saisissez manuellement l'adresse du site que vous connaissez.

8/ Imaginez que c'est le 1er Avril tous les jours ! Vérifiez l'information annoncée dans un courriel.

9/ Vérifiez que votre antivirus est interfacé avec votre programme de messagerie et qu'il gère le contenu des courriels d'une part, les pièces jointes d'autre part.

10/ Pour gagner du temps, créez des filtres : mettez en place un dossier [SPAM] dans lequel vous faites transiter automatiquement tous les messages contenant [SPAM] en objet. Vous gagnerez un temps précieux en lecture.

11/ Procédez comme ci-dessus avec les courriels provenant d'expéditeurs figurant dans votre carnet de contacts en créant un dossier [A LIRE]. Ce filtre permettra d'identifier plus rapidement les courriels « sûrs ».

12/ N'hésitez pas à vous désinscrire des nombreux emailings publicitaires non sollicités. Préférez le faire un envoyant un courriel plutôt qu'en cliquant un lien de désabonnement qui peut être un faux !

6 – Internet

- Internet est devenu incontournable : déclarations, recherches documentaires, commandes, sites internet (marchands ou vitrines), consultations, … C'est aussi un fabuleux vecteur d'attaques et d'implantation de programmes espions.

La problématique de la navigation sur internet est complexe : les navigateurs, quels qu'ils soient (Mozilla, Google Chrome, Internet Explorer), présentent des failles de sécurité, et sont régulièrement mis à jour par leurs éditeurs respectifs. Mais les navigateurs utilisent également des programmes additionnels, dits « plugins » (Java, Flash, Adobe Reader, …) qui nécessitent également une attention particulière.

Au-delà de l'outil utilisé pour naviguer, il faut également définir dans l'entreprise des règles de bonne conduite :

1/ Ne pas enregistrer ses identifiants sur les sites sécurisés.

2/ Refuser les changements de page d'accueil par défaut.

3/ Refuser les installations de barres d'outils.

4/ Ne jamais laisser un site internet juger de l'état de mises à jour de vos programmes. Ce n'est pas un site internet qui doit vous avertir qu'un programme ou plugin n'est pas à jour et vous proposer dans la foulée, de « cliquer » pour le mettre à jour. Rendez-vous plutôt sur le site de l'éditeur et téléchargez la dernière version ou bien exécutez le programme concerné et vérifiez si ce dernier propose des mises à jour.

5/ Laissez un niveau de sécurité élevé dans vos navigateurs. Préférez devoir « autoriser » la navigation sur les sites sur lesquels vous vous rendez couramment, en créant des exceptions.

6/ Lorsque vous vous connectez sur des bornes extérieures avec un appareil mobile, vérifiez que vos partages sont bloqués, n'autorisez pas le partage wifi, vérifiez les paramètres de votre firewall logiciel, et préférez les transferts de données par supports physiques (disques, clés) plutôt que par partage de dossiers.

7 – La sécurité du poste informatique

- C’est par le poste informatique que tout arrive. Entre erreur humaine, malveillance, dysfonctionnement matériel, les risques sont multiples et bien réels.

1/ La sécurité matérielle du poste est généralement assurée par la maintenance technique des équipements. C’est soit un service interne, soit un prestataire externe qui assume cette mission. Elle a pour but de maintenir un niveau de performance optimale des différents composants du poste. Les services informatiques internes, ou le prestataire, peuvent recevoir par le biais d’utilitaires installés sur un poste de travail son état de fonctionnement en temps réel et agir si besoin.

2/ Le poste de travail est protégé à minima par un antivirus et, idéalement, par une suite de sécurité intégrant : Antivirus, Antispyware, Anti-phishing, Firewall, et Antispam. Les mises à jour doivent être activées. La désactivation temporaire de la protection doit se faire avec confirmation par mot de passe.

3/ L’insertion de support USB peut être tolérée, mais l’exécution automatique des programmes doit être proscrite. De plus, une analyse avec l’antivirus du support amovible est nécessaire avant d’en récupérer les données ou d’exécuter les programmes présents sur ce support.

4/ La mise à jour des différents programmes présents sur le poste ainsi que du système d’exploitation, doit être activée. La mise à jour des programmes permet de corriger des failles de sécurité identifiées par les éditeurs.

5/ Dans la mesure du possible, aucun périphérique étranger à l’entreprise ne doit être connecté au poste. Sous prétexte d’avoir besoin de recharger la batterie d’un appareil mobile (smartphone), le simple fait de le connecter au poste pourrait permettre d’y implanter un programme malveillant ou de récupérer des données sensibles du poste.

6/ Aucun document mentionnant les mots de passe ou données confidentielles n’est « collé » sur l’écran.

7/ N’installez aucun programme promettant une amélioration des performances de votre système informatique ! Les outils nécessaires au bon fonctionnement d’un poste de travail sont déjà présents sur le poste.

8/ Pour éviter les dégâts électriques, ou une coupure de courant pouvant provoquer un dysfonctionnement dans le meilleur des cas, une perte de données dans le pire des cas, le poste de travail sera alimenté et protégé par un onduleur, qui donnera le temps à l'utilisateur d'enregistrer son travail en cours et d'arrêter le système en attendant le retour d'une ligne électrique stable.

9/ Dans certains cas, il est possible de « bloquer » une partie des droits du poste de travail, comme l'installation de programmes. Dans ce cas, on considère qu'il existe un « Administrateur » du poste qui dispose de toutes les fonctionnalités possible sur le poste et un « Utilisateur » du poste, qui exécute les programmes, mais ne peut pas en installer, limitant ainsi les risques de propagation involontaire de programmes malsains.

8 – L'utilisation des objets connectés personnels en entreprise.

- Traditionnellement appelé « BYOD », de l'anglais « Bring your own device », signifiant « apportez vos appareils personnels ».

C'est la tolérance ou l'avantage qu'a une entreprise de permettre à un salarié de connecter un de ses équipements personnels (Portable, tablette, smartphone) au réseau de l'entreprise. Soit à des fins personnelles, soit à des fins professionnelles.

Les smartphones sont très utilisés en entreprise et sont connectés au réseau wifi mis à disposition par l'entreprise. Ces appareils sont rarement protégés, les protections restant sommaires voire inexistantes.

Autoriser la connexion d'appareils personnels au réseau de l'entreprise impose de vérifier leur niveau de protection. De plus, ces appareils étant, par essence, propriété du salarié et non de l'entreprise, il n'est pas possible pour un employeur de vérifier quelles données sont présentes sur ces appareils.

Dans le cadre d'une telle tolérance, plusieurs règles sont de rigueur :

1/ Vérifier le niveau de protection de l'appareil

2/ Engager avec l'ensemble du personnel une démarche éthique, allant jusqu'à la signature d'une charte de « bonne conduite »

3/ Si l'usage est toléré pour convenance personnelle (appareil utilisable uniquement lors d'une pause ou dans certains lieux, tels que réfectoire, cantines, salle de repos, espace fumeurs), alors il convient d'isoler le réseau permettant la connexion wifi du reste du réseau de l'entreprise.

4/ Si l'usage est toléré pour convenance professionnelle, (appareil personnel utilisé en remplacement d'un matériel d'entreprise momentanément défectueux), il s'agira de vérifier l'état général du poste ainsi que son intégrité, avant de le connecter au réseau professionnel.

5/ Grand nombre d'applications installées sur les smartphones et tablettes récupèrent énormément de données : Géolocalisation, Accès aux données personnelles tels que N° de téléphone, ensemble des contacts

enregistrés dans l'appareil, appels téléphoniques, photos, habitudes de navigation… Une fois connecté au réseau professionnel, d'autres données, (celle de l'entreprise), peuvent devenir accessibles pour ces applications. Il est donc particulièrement important de vérifier quelles applications sont installées sur ces appareils et quels sont les droits que s'octroient ces applications.

6/ Il est nécessaire de scinder partie personnelle et partie professionnelle. Aucun courriel professionnel ne doit être transféré sur une adresse courriel personnelle. De même, l'appareil utilisé en entreprise ne doit pas être utilisé pour consulter des sites ou serveurs cloud personnels.

Une entreprise peut donc tolérer l'usage d'objets numériques personnels en son sein, mais il est préférable d'isoler ces appareils du réseau professionnel.

9 – La sécurisation du réseau externe de l'entreprise

- Tout comme l'entreprise a une adresse physique permettant à une personne mal intentionné de s'y introduire, le réseau informatique de l'entreprise dispose aussi d'une adresse (via le biais de sa connexion internet) et cet accès externe permet de s'introduire « virtuellement » dans l'entreprise.

Le firewall : un mur de feu infranchissable ?

Aucun acteur de sécurité informatique digne de ce nom ne serait capable d'écrire noir sur blanc qu'un firewall est infranchissable. Ou bien ce serait un menteur !

Le firewall physique (appareil analysant et régulant l'intégralité du trafic entrant depuis l'extérieur et dirigé en direction de l'entreprise) reste cependant une protection efficace, dès lors que des règles strictes sont appliquées.

Les firewalls sont également capables de gérer l'intégralité du trafic sortant.

Traditionnellement plus efficace qu'un firewall intégré à un logiciel antivirus, le firewall physique, connecté en amont du réseau informatique, représente un bouclier entre le monde extérieur et l'entreprise. Associé à des services de réseaux virtuels, de zones sécurisées, zone DMZ, internet… l'accès n'en sera que plus difficile pour les cybercriminels.

Parallèlement à cette protection qui devrait être considérée comme indispensable et obligatoire dans toutes les entreprises, et déjà évoqué, il convient de s'assurer qu'aucun matériel « administrable » à distance n'est resté dans sa configuration d'origine : les mots de passe et protocoles d'accès doivent être verrouillés.

Il convient de surveiller de manière régulière les remontées d'informations des firewalls (logs), qui sont un bon indicateur du nombre de tentatives faites pour entrer sur le réseau d'une entreprise et éventuellement découvrir par quel biais.

En effet, la question n'est pas de vérifier si une tentative d'attaque a eu lieu, car c'est quasiment une certitude, mais plutôt de vérifier comment ont réagi les systèmes de sécurité mis en place.

10 – Ne pas laisser de traces

- En agissant comme agiraient les cybercriminels (laisser le moins de traces possibles), vous sécurisez votre environnement numérique (et votre vie privée).

1/ Videz l'historique des navigateurs internet.

2/ Ne laissez pas un navigateur internet mémoriser les mots de passe.

3/ Lors de la navigation sur internet, choisissez le mode navigation privée.

4/ Ne laissez aucun fichier contenant vos mots de passe sur le poste de travail.

5/ Automatisez les tâches de suppression des fichiers temporaires.

6/ Si besoin, cryptez et protégez par mot de passe les documents sensibles, après avoir pris soin de réaliser une sauvegarde externalisée du document original non crypté.

7/ Ne laissez pas les sites internet vous pister : videz de manière régulière « le cache » du navigateur. Mieux : activez la suppression du cache lors de la fermeture du navigateur.

8/ Choisissez plutôt une version optimale et sécurisée d'un navigateur, comme Firefox ESR plutôt que Firefox.

11 – Bien choisir ses partenaires

- Avec vous, votre prestataire informatique (ou service informatique interne s'il existe), est celui qui va détenir l'ensemble des informations liées à votre structure informatique. Quelques fois il disposera également de l'ensemble ou d'une partie de vos identifiants et mots de passe. Il est donc important de s'appuyer sur un partenaire de confiance.

Dans la cadre d'un partenariat avec un prestataire il est important, voire obligatoire, de vérifier que son niveau de sécurité est 2 fois supérieur au vôtre ! Il va détenir l'ensemble des informations de vos équipements numériques. S'il est victime d'une attaque majeure, vos données nécessaires à la maintenance, stockées chez ce prestataire, deviennent donc exposées. Il doit donc répondre à l'ensemble des critères de sécurité que vous avez définis.

Un partenaire de confiance : le prestataire qui gère vos infrastructures numériques dispose très souvent d'un accès en télémaintenance sur l'ensemble de votre parc informatique. Il a donc accès à l'intégralité des données d'une entreprise. Dans ce cadre, un prestataire sera donc choisi avec le plus grand soin. Un contrat de confidentialité peut (doit) exister entre vous et lui.

Certains prestataires sont affiliés à des réseaux professionnels. C'est un gage de qualité et de confiance, ces réseaux imposant à leurs affiliés des compétences techniques et proposent régulièrement des formations techniques certifiantes liées aux services informatiques. Privilégiez donc un acteur dont les compétences sont reconnues et validées par ses pairs.

12 – Se poser les bonnes questions

- Définir une politique de sécurité, c'est se poser les questions sur le niveau de probabilité de menace, les risques encourus, et le comparer aux solutions mises en œuvre.

Complétez les tableaux ci-dessous *en les remplissant avec la valeur « 1 » dans chaque case correspondant à votre cas. (1 seule réponse par ligne), et reportez le total en dernière ligne.*

Niveau de probabilité de menaces :

Niveau de menace	Menace forte	Menace moyenne	Menace faible	Aucune menace (ou improbable)
Intrusion physique dans les locaux et/ou incendie				
Panne disque dur				
Panne générale du système informatique				
Attaque cybercriminelle				
Total Tableau 1				

Risques encourus :

Niveau de risque	Risque fort	Risque moyen	Risque faible	Aucun risque (ou improbable)
Vol du matériel informatique				
Perte de données définitive (Absence de sauvegarde externe)				
Impossibilité de poursuite d'activité rapidement				
Fuite de données confidentielles, et/ou mise hors service du système (Absence de protection Firewall)				
Total tableau 2				

Solutions mises en place :

Niveau de sécurité	Aucune solution	Solution faible	Solution moyenne	Solution forte
Protection des locaux (alarme, vidéo surveillance)				
Existence de sauvegardes fiables externalisées				
Plan de reprise d'activité				
Désactivation des accès Wifi				
Gestion de réseaux virtuels (Vlan)				
Connection de smartphones et appareils personnels				
Protection contre les accès Internet externes				
Politique interne de l'entreprise en matière de sécurité				
Mots de passe forts				
Audits et contrôles de sécurité réguliers				
Personnel de l'entreprise formé sur la sécurité et informé des risques				
Total Tableau 3				
Total tableau 1+2+3				

Total obtenu colonnes 1 + 2 : ☐ Total obtenu 3 + 4 : ☐

Analyse de votre score.

- Si le total obtenu dans les 2 premières colonnes est supérieur au total obtenu dans les colonnes 3 et 4, il est alors impératif que la question de la sécurité informatique soit étudiée rapidement et que des actions soient programmées pour restreindre les risques existants.
- Si le total obtenu dans les 2 premières colonnes est quasi équivalent au total obtenu dans les colonnes 3 et 4, alors des solutions ont déjà été mises en place et il reste soit à les améliorer soit à couvrir les risques qui n'ont pas encore été pris en compte.
- Enfin si le total obtenu dans les colonnes 3 et 4 est largement supérieur au total obtenu dans les colonnes 1 et 2, le risque numérique est déjà pris en compte et des solutions fortes existent. Un audit de sécurité confirmera ces bonnes pratiques.

13 – En cas de doute

- Un poste informatique présente un comportement inhabituel, des éléments ont disparu ou sont apparus, le poste est très lent, des utilisateurs reçoivent des mails de votre part alors que vous n'avez rien expédié ?

Le premier conseil en cas de doute est d'isoler le poste concerné en le déconnectant du réseau.

Il faut ensuite procéder à une sauvegarde rapide du poste (pour une fois un support USB sera toléré) et uniquement des documents récents et importants qui n'auraient pas encore fait l'objet de sauvegarde.

C'est seulement après cette étape que le poste pourra être éteint, de manière brutale (coupure par le bouton de mise en marche), et ne devra plus être rallumé, pour que d'éventuelles traces d'attaque ne soient pas souillées par une remise en route du poste.

Il convient ensuite d'avertir les responsables informatiques et, s'il existe, le prestataire, qui pourront procéder à l'analyse des données du disque et remettre en état le poste de travail, après s'être assurés que les sécurités sont opérationnelles.

Au retour en exploitation du poste (ou avec un autre poste sain), il s'agit de modifier l'ensemble des mots de passe qui étaient en service sur le poste suspect.

Enfin, il s'agira de vérifier que les données restaurées sont exploitables (leur intégrité aura été vérifiée préalablement à leur restauration sur le poste).