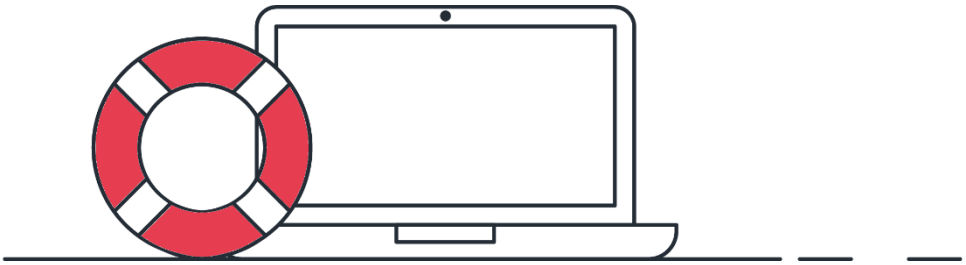
CLOUD & SERVEURS INFOGÉRÉS

Les 10 commandements de la sécurité informatique



Agence de Paris (Siège social)
70 rue Berthie Albrecht
94400 Vitry-sur-Seine

Téléphone : 01 40 64 01 31

Agence de Lyon
44 ancienne route d'Irigny
69530 Brignais

Téléphone : 04 26 46 39 84

Préambule

Dans un monde de plus en plus connecté, la sécurité des données est devenu un enjeu majeur pour les sociétés. **Malheureusement de nombreuses personnes pensent qu'un hack n'arrive qu'aux autres.** Aujourd'hui, tous les ordinateurs sont reliés entre eux, les salariés et dirigeants laissent des informations sur les réseaux sociaux favorisant le social hacking, les objets connectés se multiplient tout comme les risques de fuites de données. Dans ces conditions, il est nécessaire de rappeler les précautions de bases à prendre, parfois techniques mais toujours de bon sens.

1. Jamais tes mots de passe, tu ne négligeras.

« J'ai des mots de passe pour tout, mon ordinateur, mes comptes bancaires, ma messagerie, j'ai trouvé la solution, je mets le prénom de ma fille partout ! Elle s'appelle Léa ».

Est-il vraiment nécessaire de préciser qu'il s'agit d'une mauvaise idée ? Un mot de passe sécurisé contient des chiffres, des lettres (majuscule et minuscule), des symboles spéciaux et 8 caractères au minimum. Les hackeurs utilisent des routines qui vont générer des mots de passe en rapport à des mots du dictionnaire, des prénoms ou en testant toutes les combinaisons de lettres. En cas de suspension de l'accès pendant X minutes, même après plusieurs tentatives, la routine peut s'exécuter pendant des mois sans que personne ne s'en aperçoive.

Notre conseil : Utiliser un mot de passe complexe mais facilement retrouvable grâce à un moyen mnémotechnique._Vous êtes né en 1988 ? Vous êtes vivez dans le Morbihan et votre femme s'appelle Lori ? Et si vous utilisiez le mot de passe 88#LoRi*56 ? Inoubliable, même en cas de divorce. C'est un bon début mais pas encore suffisant. Si vous utilisez le même mot de passe partout, une fuite de données sur un site e-commerce mal sécurisé peut alors aboutir à la divulgation de tous vos accès.

Allons un peu plus loin : vous pouvez avoir des mots de passe uniques en toute simplicité. Vous utilisez LinkedIn ? Ajoutez un « L » majuscule à votre mot de passe L*88#LoRi*56. Facebook ? Un « F », F*88#LoRi*56. Vous pouvez ainsi personnaliser votre mot de passe en fonction des services auxquels vous accédez. Avantage non négligeable : plus jamais vous n'oublierez le mot de passe de vos réseaux sociaux ou messagerie.

2. Ta vie privée, tu protégeras.

« *Dans les Caraïbes pour deux semaines ! Pas de mail, pas de PC !* » nous indique Thierry sur sa page Facebook. Quelle chance Thierry ! En plus, quand on dirige une PME à succès, comme lui, ces deux semaines de vacances sont bien méritées. Pour autant était-il vraiment judicieux d'informer le monde entier de son absence et donc de son incapacité à joindre ses collaborateurs pour les jours à venir ? Probablement pas. Si c'est le meilleur moment pour cambrioler sa résidence principale, c'est également le meilleur moment pour s'attaquer à sa société via le social hacking.

Vous seriez étonné du nombre de collaborateurs qui « pour bien faire » sont capables de donner un mot de passe par téléphone à un inconnu ou de faire un virement de plusieurs milliers d'euros sur un compte bancaire, dans les Caraïbes justement. Pour cela, il suffit d'être un « supposé ingénieur » de la société de maintenance informatique : *« Thierry est au courant de mon intervention oui, mais je n'ai pas son mot de passe* » ou encore Thierry

lui-même « *Je n'arrive pas à me connecter depuis mon lieu de vacances ! Vous pourriez voir avec le DSI pour réinitialiser mon login et mon mot de passe ?* ».

Notre conseil : **dirigeants, cadres ou employés, veillez à ne pas divulguer sur les réseaux sociaux des informations telles que votre incapacité à gérer une situation de crise ou vos difficultés à être joint par vos collaborateurs.**

A titre d'exemple, les infrastructures de Celeonet font l'objet d'attaques régulières. Les pics d'attaques ont lieu systématiquement durant les vacances de Noël et le mois d'Août, périodes où les hackers supposent que de nombreux personnels sont en congés et que notre réactivité est moindre… perdu !

3. Tes collaborateurs, tu sensibiliseras.

Même sur le système informatique le plus sécurisé du monde, il restera toujours une faille : elle se situe entre la chaise et le clavier, son nom ? L'utilisateur. Il est humain, c'est un être avec ses qualités, ses défauts, ses trous de mémoire (qu'un post-it avec son login et son mot de passe collé à son écran permet de combler) et ses bourdes : « *Je suis désolé je ne savais pas que c'était un serveur, sinon je ne l'aurais pas débranché pour charger mon téléphone portable* ».

Il est important de sensibiliser, voire de former, l'ensemble des utilisateurs aux risques informatiques. Cela devrait commencer dès l'arrivée d'un nouveau collaborateur par la lecture et la signature de la charte informatique de la société. Charte qui reprend les droits et les devoirs du salarié, la politique de mot de passe, une sensibilisation sur les virus, spams et autres joyeusetés liées à la messagerie.

Ne sombrez pas dans la paranoïa : *« Les hackers sont partout ! Ils nous attaquent en permanence !! ».* Bon c'est vrai, mais sensibiliser ne veut pas dire terrifier.

Notre conseil : **Sensibilisez vos utilisateurs sur les risques liés à l'informatique et à la perte de données, sans sombrer dans la paranoïa. J'allais oublier, jamais au grand jamais, un accès administrateur à la machine locale ne doit être laissé à une personne non-habilitée. Cela vous semble évident ? Et pourtant dans nombre d'entreprises c'est le cas. Cela simplifie l'ajout d'un plugin flash, la mise à jour de cette maudite machine virtuelle Java etc… Le problème est que vous retrouverez dans un laps de temps relativement court, tout ce que le net compte de freewares et de logiciels d'évaluation sur cet ordinateur. Au fait : saviez-vous que l'essentiel des virus, chevaux de Troie et autres logiciels malveillants proviennent de freeware ? Vous venez d'ouvrir en grand la porte de votre système informatique.**

4. Des configurations par défaut, tu te méfieras.

« *La plupart des périphériques fonctionnent tout seul, il suffit de les brancher et c'est parti ! C'est à se demander à quoi sert un informaticien !* ». Soyons clair : plus un équipement est simple à installer, moins il est sécurisé. Cela tient simplement au fait qu'en s'abolissant des contraintes de sécurité, le constructeur n'a pas à se soucier de la topologie de votre réseau ; « *tu branches, ça marche. MAG-NI-FI-QUE !* »

Prenons quelques exemples concrets : chaque matériel a une adresse sur votre réseau, il s'agit d'une adresse IP. Lorsque vous installez une imprimante dans votre société, cette dernière récupère une adresse IP via DHCP et s'installe en quelques clics grâce à l'auto-détection. Aujourd'hui toutes les imprimantes disposent d'une interface d'administration web avec un login et un mot de passe par défaut. Ces dernières sont très complètes ; elles permettent de rediriger les flux d'impression à travers internet, de paramétrer l'imprimante etc… Vous pouvez également fixer une nouvelle adresse IP, une personne malintentionnée peut mettre la même adresse que celle du PC du DG ou de Vanessa de la comptabilité : désorganisation ou vol de documents assuré avec une simple imprimante.

« *Oui mais encore faut-il accéder au réseau de l'entreprise* » me direz-vous ? Ce à quoi je vous répondrai : « *votre box internet, il vous a suffi de la brancher pour vous connecter à Internet ? Aussi simplement qu'une imprimante ? Votre box a également une interface web et un mot de passe par défaut.* » Quant au wifi toujours activé, il est possible de cracker une clé wifi en quelques minutes.

Notre conseil : **Quel que soit l'équipement que vous branchez sur votre réseau, changez les logins et mots de passe par défaut et désactivez les services inutiles. Ces quelques dizaines de minutes ne sont pas perdues. J'oubliais, « *savez-vous que votre téléphone IP a une interface web d'administration avec un login et un mot de passe par défaut ?* » Il est on ne peut plus simple d'utiliser votre ligne pour téléphoner à l'autre bout du monde.**

5. Tes tests, en sureté tu mettras.

Qu'il s'agisse du développement d'un logiciel, d'un site internet ou d'un équipement réseau, effectuer des tests hors d'un environnement de production est logique et sain. Ce qui l'est moins, c'est de considérer qu'un test nécessite une sécurité au rabais, absence de mot de passe, visibilité du test depuis tout internet, droits étendus pour les utilisateurs etc…

La mesure de base qui doit être appliquée est la suivante : un test ne doit être accessible qu'aux personnes qui le réalisent. Vous devez faire une démonstration à votre client à distance ? Protégez à minima l'accès via un mot de passe.

Vos tests sont concluants ? C'est une bonne nouvelle. Ne commettez pas la pire des erreurs en transformant votre plateforme de test en plateforme de production. Mieux vaut repartir sur une installation propre et la paramétrer correctement, en terme de sécurité et de droits d'accès, pas à pas.

Tester avant de déployer c'est bien, réinstaller sur un environnement de production propre c'est encore mieux, mais oublier son test au fin fond d'un serveur, c'est mal, très mal et surtout excessivement risqué. Ce test peut vite se transformer en verrue cachée au sein de votre système informatique, non-monitoré, jamais mis à jour, oublié. Contrairement au vin, il ne se bonifie pas avec le temps. Il peut devenir une faille dans votre système informatique. Un test n'a pas vocation à perdurer, une fois terminé, il doit être supprimé dans sa globalité. Soyez conscient qu'internet est parcouru en permanence par des vers informatiques qui cherchent des systèmes faillibles. Vous n'êtes pas forcément ciblé initialement mais la présence de failles dans votre système d'information vous rend intéressant pour un hackeur lambda.

Notre conseil : **La sécurité d'un outil ou d'un système en test ne doit pas être négligée. Un test n'a pas vocation à devenir une plateforme de production ou à perdurer dans le temps. Une fois votre système fonctionnel, votre test doit disparaitre. Dans le cas particulier des applications web, privilégiez l'utilisation d'un serveur de développement distinct de la production. Il existe de nombreux outils qui vous faciliterons la vie, tout en garantissant la sécurité de votre plateforme.**

6. Tes systèmes informatiques, tu éteindras (en plus c'est bon pour la planète).

Il y a bien longtemps, j'ai côtoyé un responsable sécurité qui avait conclu une discussion par cette phrase : « *Le seul système informatique infaillible, c'est celui qui est éteint* ». Phrase pleine de sagesse, mais un peu extrême peut-être. Nos utilisateurs de l'époque n'étant pas tout à fait enthousiastes à l'idée de remplacer leurs ordinateurs par un bloc de papier et un crayon.

Confrères informaticiens, ne déposez pas immédiatement vos CV dans les papeteries des alentours. Comme j'ai pu le dire précédemment, aujourd'hui nous vivons dans un monde hyper connecté : ordinateurs, tablettes, téléphones, etc… Tous nos périphériques sont connectés à Internet et à notre système d'information. Faut-il tout éteindre ? Bien-sûr que non. Faut-il limiter les points d'entrée lorsqu'ils ne sont pas utilisés ? Oui, c'est une question de bon sens.

Tous ces périphériques sont autant de portes d'entrée sur le système d'information de l'entreprise. La plus visible et la plus dangereuse : cet ordinateur laissé sans surveillance, session ouverte et non verrouillée. Quand le matériel informatique n'est pas utilisé, au pire on le verrouille, au mieux on l'éteint, à plus forte raison quand il est 18h00 et que la journée est terminée.

Outre le fait qu'il ne faut pas de consommer de l'électricité pour rien, un ordinateur allumé est également un système informatique sur lequel il est possible de se connecter à distance s'il présente des failles. Ne pas maintenir les systèmes informatiques non utilisés en fonctionnement c'est également réduire le risque d'être détecté comme une cible potentiel par un hacker.

Notre conseil : **Ne laissez pas vos périphériques allumés lorsqu'ils ne sont pas utilisés. Votre facture d'électricité ne s'en portera que mieux et cela limitera également le nombre d'accès possible à votre système d'information.**

7. De choisir les bons prestataires, tu t'assureras.

De plus en plus d'entreprises font appel à un prestataire, que ce soit pour le développement de leur site internet, la gestion de leur système informatique ou la fourniture de services d'hébergement ou de messagerie.

Mais connaissez-vous l'expression suivante ? « *Quand c'est gratuit, c'est vous le produit* ». Elle s'applique tout particulièrement au monde de l'internet. Votre personnalité fait de vous un produit que Facebook et Google aime connaitre pour mieux vendre vos informations.

Il n'y a rien de gratuit en ce bas monde, à commencer par les solutions de stockage en ligne ou de messagerie. Vous éviterez donc scrupuleusement de confier des données confidentielles telles que vos emails ou fichiers de travail à des sociétés dont la source de revenu est le profilage.

Le choix d'un prestataire informatique n'est pas anodin. C'est une relation qui doit être basée sur la confiance mutuelle, et à première vue, ce n'est pas aussi simple qu'on pourrait le croire. Assurez-vous de ses références et de ses compétences, le bouche à oreille a encore de belles années devant lui. Faites-vous conseiller par votre réseau et utilisez societe.com pour vous assurer de la solidité financière de votre nouveau « partenaire ».

Dans la mesure du possible, vous ferez travailler vos prestataires sur des jeux de données anonymisés et vous vous assurerez de ne leur laissez aucune donnée une fois la prestation terminée. Vous seriez surpris du pourcentage de clients qui laissent toutes leurs données chez leur hébergeur à la clôture de leur contrat. Alors, une idée ? Pas loin de 95%.

Notre conseil : **Le bouche à oreille n'est pas mort, c'est bien souvent votre réseau qui vous permettra de trouver de bon prestataire. Les réseaux sociaux permettent également de juger du sérieux des « nouveaux entrants », quant à societe.com, il vous permettra de valider la pérennité de votre relation avec votre nouveau prestataire. Préférez les sociétés françaises ou européennes, en cas de déconvenue vous serez plus apte à faire valoir vos droits ou à trouver un arrangement.**

8. Tes sauvegardes, tu vérifieras.

Tout le monde sauvegarde ses données, posez la question autour de vous, vous verrez. Du particulier à l'entreprise, c'est un principe appliqué par tous. Si vous creusez un peu, vous constaterez que tout le monde a l'intention de sauvegarder ses données « *j'ai un disque dur externe, je dois m'en occuper* » « *Windows le fait tout seul non ?* » « *Oui, j'ai copié toutes mes données sur une clé USB il y a 6 mois… mais je crois que mon fils a mis un film dessus* ».

Quant aux entreprises, il y a une règle invariable que j'ai pu constater à de multiples reprises : quand vous avez besoin d'un backup, c'est en général à ce moment-là que vous constatez que l'utilitaire de sauvegardes a cessé de fonctionner il y a quelques mois, sans même avoir la décence de vous en informer. Les ennuis commencent. Passons sur le cas des particuliers, les photos du petit dernier ont rejoint le cimetière des disques durs, c'est frustrant mais cela n'est pas dramatique.

Le cas des entreprises est bien plus critique : la perte de données peut perturber gravement le fonctionnement d'une entreprise, voire l'amener à la liquidation. De fait, il est important de s'assurer que nos données sont sauvegardées en toute sécurité. Il faudra bien-entendu éviter d'utiliser un NAS dans les locaux de l'entreprise, un voleur ou un incendie faisant rarement le nécessaire pour vous laisser un jeu de sauvegardes exploitables.

Il est nécessaire de mettre en place une politique de sauvegarde, idéalement avec un stockage distant, et une politique de vérification. Un simple mail matinal est déjà une excellente solution, une petite vérification approfondie une fois par mois vous permet de vous affranchir des problèmes qui pourraient passer inaperçus.

Evitez cependant les solutions gratuites sur internet ; vos données ont de la valeur pour vous mais également pour d'autres. Inutile d'en donner l'accès à n'importe qui, à plus forte raison à des sociétés basées aux Etats Unis. Ces dernières ont une vision très différente de la notion de confidentialité, telle que nous la concevons en Europe.

Notre conseil : **Mettez en place une politique de sauvegardes automatisées de vos données, avec un rapport d'exécution quotidien. Externalisez ces données vers un tiers de confiance. N'hésitez pas à faire un test de restauration une fois par an afin de vous éviter toute mauvaise surprise.**

9. D'un bon antivirus, tu t'équiperas.

Il y a quelques années, les antivirus avaient pour réputation de faire chuter les performances des ordinateurs et c'était vrai. Aujourd'hui, avec l'essor d'internet, la plupart effectuent un scan des données échangées en temps réel. Ils ne souffrent plus de lourdeur et se mettent à jour automatiquement, de façon transparente.

Nous utilisons tous des boîtes mails et il s'agit probablement là du plus grand pourvoyeur de virus informatiques de tous les temps. Assurez-vous que vos serveurs de messagerie sont équipés d'antivirus et d'antispams qui procéderont à la suppression des fichiers vérolés, avant même qu'ils ne vous atteignent. En complément, un antivirus local supprimera les derniers virus qui n'auraient pas été détectés par le serveur.

Il faut savoir que nos ordinateurs sous Windows, tablettes et téléphones sont vulnérables aux attaques virales et qu'il existe pour tous des solutions antivirales gratuites ou payantes. Les serveurs sous Linux ou Unix sont quant à eux, sont moins concernés par ce type de problèmes, mais restent tout de même vulnérables.

Notre conseil : **Ne vous privez jamais de la sécurité d'un antivirus, cela vous évitera de nombreux désagréments tels que la fuite de données ou des perturbations de votre système informatique. Un antivirus permettra également de détecter les chevaux de Troie ou autres logiciels n'ayant pour seul objectif que de capter vos données et de les transmettre à un tiers.**

10. Du monde entier, tu te connecteras (tout en restant prudent)

Ma fibre d'administrateur système vibre à de nombreuses occasions : quand je visite un datacenter, quand nous réceptionnons des serveurs versions « bêtes de compet' » mais également quand s'ouvre à moi de nouvelles opportunités pour accéder à mes données ou à mon environnement informatique, où que je sois dans le monde.

Le développement du télétravail, l'utilisation de terminaux distants sur les chantiers, l'itinérance des commerciaux ou les grèves de la SNCF sont autant de paramètres qui font que, de plus en plus d'utilisateurs se connectent au système informatique de leur société de l'extérieur des locaux.

Certaines précautions sont cependant à prendre pour ne pas ouvrir une porte béante dans tous les systèmes de sécurité de l'entreprise et faciliter l'intrusion de personnes malveillantes. Tout d'abord il est évident que cette connexion ne doit pas être réalisée depuis un périphérique dont nous n'avons pas la maitrise, depuis un cybercafé par exemple ou un ordinateur en libre accès. Ces derniers peuvent être équipés de sniffeurs ou être contaminés par un cheval de Troie.

L'accès au réseau de l'entreprise doit impérativement s'effectuer à travers un canal sécurisé et ne pas permettre qu'un utilisateur lambda puisse atteindre le système informatique. La société ne permettra donc l'accès à son réseau qu'à travers un serveur VPN avec login et mot de passe.

Notre conseil : N'utilisez que des périphériques fournis par l'entreprise pour vous connecter à distance, évitez absolument d'utiliser des ordinateurs en libre accès. Assurez-vous que le réseau de votre entreprise n'est pas visible dans sa globalité depuis internet et qu'une solution sécurisée est mise en place pour y accéder.

Pour conclure :

J'espère que ces « 10 commandements » vous seront utiles, je ne peux que vous conseiller de les appliquer et de faire vôtre l'adage « Pour vivre heureux, vivons cachés ». Moins vos systèmes informatiques seront visibles sur Internet, moins ils seront ciblés par les attaques.

Pour vos sites internet ou boutiques E-Commerces, utilisez des firewalls applicatifs ou des solutions de reverses proxies pour détourner les attaques de vos serveurs.

Celeonet développe et déploie au quotidien des solutions de sécurité pour ses clients, travaillons ensemble !