Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SÉCURITÉ INFORMATIQUE

MEMENTO CYBERSECURITÉ POUR LE CRÉATEUR D'ENTREPRISE

ÊTRE ENTREPRENEUR, C'EST...
UTILISER UN ÉQUIPEMENT INFORMATIQUE

Commencer une activité professionnelle implique le plus souvent d'être équipé en matériel informatique. Lorsqu'on fait l'acquisition d'un ordinateur, certains logiciels sont installés mais avec le temps, les éditeurs découvrent les vulnérabilités et publient des mises à jour de sécurité. Ne pas les installer, c'est laisser à l'attaquant une porte d'entrée.

PROCÉDER AUX MISES À JOUR LOGICIELLES SANS DÉLAI

Des conditions d'utilisation accompagnent certains appareils. Il convient de les respecter en évitant d'installer des logiciels non autorisés. Le respect de ces règles participe à la sécurité de vos données.

RESPECTER LES CONDITIONS D'UTILISATION DE VOS APPAREILS

Des informations confidentielles peuvent être stockées sur cet équipement. Afin de protéger vos documents en cas de vol ou d'accès physique à l'appareil, il convient de verrouiller son appareil par code ou mot de passe.

VERROUILLER L'ACCÈS À SON PROFIL UTILISATEUR

On ne peut prévoir tous les scénarios et une défaillance matérielle peut toujours arriver. Pour éviter de perdre ses documents définitivement en cas d'incident, une sauvegarde régulière est nécessaire.

SAUVEGARDER RÉGULIÈREMENT SES DONNÉES

Pour aller plus loin :
https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

...DISPOSER D'UNE IDENTITÉ NUMÉRIQUE

Le nom de domaine est la base de votre identité sur Internet: il s'agit de la partie se trouvant après l'arobase « @ » dans les adresses de courriel, la partie après www. dans les adresses de sites web.

L'usage d'un domaine se terminant en. fr permet de bénéficier des services fournit par l'AFNIC (association délégataire d'une mission de service publique) qui développe les pratiques modernes de sécurité et ancre les éventuelles disputes juridiques dans le cadre réglementaire français et européen.

SÉCURISER SON NOM DE DOMAINE

Le courriel reste le moyen de communication le plus utilisé, particulièrement en entreprise. Comme les standards techniques avant 2005 attachaient peu d'importance à la cybersécurité, les usurpations d'identité sont nombreuses. Assurez-vous que le fournisseur de votre choix a déployé tous les standards de sécurité modernes (SPF, DKIM, DMARC, STARTTLS).

Pour aller plus loin :
https://www.afnic.fr/fr/votre-nom-de-domaine/comment-choisir-et-creer-mon-nom-de-domaine/

Pour aller plus loin :
https://www.afnic.fr/medias/documents/dossiers_thematiques/AFNIC_DossierThematique_FrLock.pdf

SÉCURISEZ VOTRE IDENTITÉ PAR VOIE DE MESSAGERIE

Pour aller plus loin :
https://www.economie.gouv.fr/hfds/cybersecurite-et-politique-ministerielle-ssi

...OFFRIR DES SERVICES NUMÉRIQUES

Un site web est la vitrine de l'entreprise sur Internet. Traditionnellement, les communications entre navigateur et serveurs se déroulaient en clair sauf exception (transactions bancaires notamment). A l'usage, il est apparu que les communications en clair constituent une menace à la vie privée, voire permettent des fraudes. C'est pourquoi les navigateurs renforcent les alertes à l'égard des sites web qui n'ont pas été sécurisés en https.

Autant donc partir sur une bonne base, en créant un nouveau site web en https dès le départ.

OFFRIR À SES CLIENTS NUMÉRIQUES UN SITE INTERNET DISPONIBLE EN HTTPS

La loi informatique et libertés encadre le traitement des données personnelles. Outre l'aspect règlementaire, ces mesures sont importantes car elles valorisent la relation clientèle.

Pour aller plus loin :
https://www.cnil.fr/fr/comprendre-vos-obligations/les-principes-cles

Pensez également à la sécurité des paiements sur internet.

Pour aller plus loin :
https://www.banque-france.fr/sites/default/files/medias/documents/brochure-commercants-securite-paiements.pdf

...ÊTRE RICHE D'UN PATRIMOINE NUMÉRIQUE

Certains logiciels de traitement de texte proposent d'ajouter un code pour consulter un document. Il s'agit d'un premier niveau de sécurité. Lorsque le logiciel ne dispose pas de cette option, il est également possible de « chiffrer » le document à l'aide d'un logiciel spécifique.

VERROUILLER L'ACCÈS AUX FICHIERS CONFIDENTIELS

Pour aller plus loin :
https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

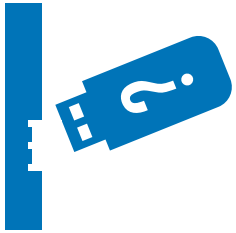
Les rançongiciels sont une menace durable.

Pour aller plus loin :
https://www.cybermalveillance.gouv.fr/wp-content/uploads/2017/01/ANSSI_ACYMA_FILM-2.webm

Pour votre entreprise, ils constitueront un risque réel ou seulement une nuisance, selon que vos données soient protégées ou non par un plan de sauvegarde.

Les désastres naturels, les vols de matériels, les erreurs humaines de manipulation des données restent aussi plus fréquentes qu'on ne veut le reconnaître.

Une pratique de base consiste à mettre en place 3 copies, 2 exemplaires localement, 1 sauvegarde sur site distant. Les pratiques avancées incluent également le chiffrement et l'historisation avec déduplication. Des outils, y compris Open Source, sont largement disponibles pour automatiser ces sauvegardes.



IMPLÉMENTER LA SAUVEGARDE 3-2-1

Si votre entreprise compte développer des savoir-faire technologiques issus de recherche, elle peut devenir une cible pour des acteurs de l'intelligence économique. A minima, elle développe une base clients qu'elle doit protéger.

Vous ne garderiez pas des papiers importants ailleurs que dans un bureau et un coffre fermé « à double tour ». L'équivalent numérique consiste à utiliser des mots de passe (l'équivalent de vos clés) et à les gérer avec des applications de gestion de « trousseaux de clés ». Ces applications sont vivement recommandées parce que nous ne savons pas bien générer des mots de passe vraiment aléatoires, ni les mémoriser, si bien que nous réutilisons, itérons des motifs communs, et un ensemble de pratiques qui ouvrent la porte aux attaquants.

Du moment que le mot de passe est fort, chiffrer les documents eux-mêmes avec les applications courantes (fichiers. docx. odf. pdf ou même. zip) forme une protection résistante.

PROTÉGER SES « SECRETS DE FABRIQUE »

EN CAS D'INCIDENT

Si, malgré vos précautions, vous êtes victime d'un incident de cybersécurité, le Groupe d'Intérêt Public ACYMA a mis sur pied le site www.cybermalveillance.gouv.fr pour mettre en relation entreprises, prestataires spécialisés et organismes compétent proches de chez vous.

En cas d'atteinte aux personnes ou aux biens, il est de votre responsabilité de porter plainte.

En cas d'incident
https://www.cybermalveillance.gouv.fr

Signaler un contenu illicite
https://www.internet-signalement.gouv.fr

Signaler un contenu illicite
http://www.pointdecontact.net

SG
Secrétariat général

HFDS Bercy

Secrétariat Général
139-145 rue de Bercy, PARIS
Septembre 2017