Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

SÉCURITÉ INFORMATIQUE

MEMENTO CYBERSECURITÉ POUR LE DIRIGEANT D'ENTREPRISE

ÊTRE DIRIGEANT...
C'EST ORGANISER LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DE SON ENTREPRISE

Une entreprise a vocation à créer de la valeur ajoutée. Afin de protéger la création de valeurs, le dirigeant prend les mesures nécessaires pour organiser la cybersécurité de son entreprise.
La responsabilité est attribuée à un responsable de la sécurité des systèmes d'information (RSSI) qu'il convient donc de désigner. Selon la dimension de l'entreprise et la sensibilité des données traitées, une équipe dédiée à la SSI est à considérer. Les comparaisons internationales permettent de recommander d'affecter au moins 5% des effectifs informatiques à la cybersécurité.

DÉSIGNER UN RSSI ET, LE CAS ÉCHANT, CONSTITUER UNE ÉQUIPE DÉDIÉE

Pour aller plus loin :
https://syntec-numerique.fr/sites/default/files/Documents/Medef_Syntec_2_-_Nommer_un_responsable_securite_numerique.pdf

Il est nécessaire d'informer les employés des conditions d'utilisation des moyens informatiques au sein de l'entreprise. Pour ce faire, une charte informatique est nécessaire.

Pour aller plus loin :
https://www.cnil.fr/sites/default/files/typo/document/20100730-MOD-CHARTE_INFORMATIQUE_CIL-VD.pdf

Les stagiaires et prestataires doivent également respecter les conditions d'utilisation de ses systèmes d'information. L'ensemble des personnels doit faire l'objet d'une sensibilisation régulière.

...C'EST 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 (ex. : frlock) et ancre les éventuelles disputes juridiques dans le cadre réglementaire français et européen.

L'AFNIC accompagne aussi les grandes organisations pour créer des domaines spécifiques (ex. : .paris), ce qui montre l'importance de maîtriser ses marques dans l'espace numérique.

Sécuriser son nom de domaine
https://www.afnic.fr/medias/documents/Dossiers_pour_breves_et_CP/afnic_dossier-thematique-securiser_VF.pdf
https://www.afnic.fr/medias/documents/dossiers_thematiques/AFNIC_DossierThematique_FrLock.pdf

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; vous pouvez être victime de fraudes comme les « fraudes aux président ».

Pour aller plus loin :
http://www.ccampuslearn.net/TRANSIT/CDSE/2012746_we_14/story.html

Assurez-vous que le fournisseur de votre choix a déployé tous les standards de sécurité modernes (SPF, DKIM, DMARC, STARTTLS).

SÉCURISEZ VOTRE IDENTITÉ PAR VOIE DE MESSAGERIE

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

...C'EST 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 pour la vie privée, voire permettent des fraudes. C'est pourquoi les navigateurs renforcent les alertes à l'égard des communications non disponibles en https c'est-à-dire non sécurisés.

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

OFFRIR À SES CLIENTS DES SERVICES NUMÉRIQUES UNIQUEMENT DISPONIBLES EN HTTPS

Les technologies utilisées sur l'internet évoluent rapidement. Lorsqu'un site internet est créé, une revue régulière de sécurité doit être programmée, notamment au regard des exigences portées par les navigateurs.

PRÉVOIR UNE REVUE RÉGULIÈRE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Préparez également votre entreprise au règlement européen sur la protection des données

Pour aller plus loin :
https://www.cnil.fr/fr/principes-cles/reglement-europeen-se-preparer-en-6-etapes

...C'EST ÊTRE RICHE D'UN PATRIMOINE NUMÉRIQUE

Certaines informations sont plus importantes que d'autres et des mesures adaptées s'appliquent. Dans un premier temps, un marquage de l'information selon sa sensibilité est un premier pas nécessaire. Les critères découlent d'une analyse de risque.

Pour aller plus loin :
https://syntec-numerique.fr/sites/default/files/Documents/Medef_Syntec_1_-_Identification_des_risques.pdf.

MARQUER L'INFORMATION SENSIBLE

Les rançongiciels constituent 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 une politique 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.

Un système de gestion de sauvegarde est nécessaire mais ne suffit pas. Une politique de continuité infor-

matique est nécessairement définie afin de conserver une activité minimale en cas d'incident et permettre un rétablissement normal au plus vite.

DÉFINIR UNE POLITIQUE DE CONTINUITÉ INFORMATIQUE

Si votre entreprise développe 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.

La création, le stockage, l'échange d'information sensible sont réalisés au moyen de solution de chiffrement.

PROTÉGER SES « SECRETS DE FABRIQUE »

Le mot de passe est un système d'authentification insuffisant lorsqu'un employé a accès à une information sensible. Il est alors préférable de privilégier un moyen d'authentification « fort » au moyen d'une carte à puce contenant un certificat numérique.

L'ACCÈS À L'INFORMATION SENSIBLE EST RÉALISÉ AU MOYEN D'UN CERTIFICAT NUMÉRIQUE

La protection du potentiel scientifique et technique de la France fait aussi l'objet d'une politique spéciale. Elle vise en particulier à protéger physiquement les laboratoires de recherche qui participe au patrimoine scientifique français.

Pour aller plus loin :
www.sgdsn.gouv.fr/uploads/2016/12/a5-ppst-hd.pdf

Un recueil de cas pratiques cyber a été réalisé par la DGSI.

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

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

Contact DGSI :
securite-economique@interieur.gouv.fr

SG
Secrétariat général

HFDS Bercy

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