Cybersécurité

Votre entreprise est-elle prête ?

economie
SPF Economie, P.M.E., Classes moyennes et Energie

.be

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Service public fédéral Economie, P.M.E., Classes moyennes et Energie
Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
https://economie.fgov.be

tél. 0800 120 33 (gratuit)

facebook.com/SPFEco

@SPFEconomie

youtube.com/user/SPFEconomie

linkedin.com/company/fod-economie (page bilingue)

Editeur responsable : Jean-Marc Delporte
Président du Comité de direction
Rue du Progrès 50
1210 Bruxelles

Version internet

209-18

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Table des matières

1. Introduction

Donner une bonne image de votre entreprise sur internet est capital.

Etre présent sur le web, que ce soit simplement pour faire connaître votre entreprise ou pour y vendre vos services ou vos biens, représente une source essentielle de redynamisation et de croissance.

En effet, maîtriser votre image sur le web déterminera en grande partie vos relations avec vos partenaires professionnels ainsi qu'avec vos clients finaux.

Vos futurs partenaires professionnels chercheront à obtenir des informations sur votre entreprise avant de conclure un contrat avec vous, il est donc essentiel de développer un site web professionnel et de maîtriser votre image. En sécurisant votre site et vos données de manière efficace, vos partenaires seront rassurés et passeront plus facilement un contrat avec vous car leur sécurité peut également dépendre de la vôtre...

S'assurer d'avoir des partenaires de confiance qui maîtrisent leur environnement informatique est de plus en plus crucial pour chaque entreprise.

Par ailleurs, de plus en plus de consommateurs effectuent des recherches en ligne avant de réaliser un achat en magasin ou sur internet. Votre e-réputation est donc primordiale.

Parmi les motifs qui poussent les consommateurs à franchir le cap de l'achat en ligne, citons notamment :

- les aspects pratiques (commande à toute heure de la journée, délais de livraison…) ;
- les prix (plus faciles à comparer en ligne) ;
- le choix ;
- la qualité des informations fournies (description du produit, avis d'autres consommateurs, explications par rapport au remboursement éventuel, aux délais de livraison, à la garantie…).

En revanche, parmi les facteurs fréquemment cités comme un frein à l'achat en ligne pour les consommateurs figure principalement l'absence de confiance quant à la sécurité des informations mises en ligne. En 2016, un internaute sur cinq a décidé de ne pas acheter en ligne des biens ou des services destinés à un usage privé, en raison de craintes liées à la sécurité. Les consommateurs ont notamment peur que leurs données personnelles soient utilisées de manière frauduleuse et que leurs données bancaires soient volées.

Dans ce cadre, disposer de bonnes mesures en matière de sécurité de l'information et le faire savoir aux consommateurs permet de les rassurer et favorise l'augmentation du volume de transactions.

Etre présent sur le web offre de nouvelles opportunités pour les entreprises mais demande également de développer une stratégie numérique qui comprend des mesures de protection nécessaires.

En effet, quelle que soit la taille de votre entreprise, les cyberattaques sont souvent synonymes de perturbations désagréables voire de pertes sévères que ce soit en termes :

- d'atteinte à l'image et de perte de confiance du monde extérieur ;
- de destruction et/ou de vol d'informations commerciales clefs ;
- d'indisponibilité du site officiel ou de dégradation de l'outil de travail à la suite de certaines cyberattaques ;
- de sanctions éventuelles, par exemple, en cas de fuite de données à caractère personnel, etc.

A chaque incident, les conséquences financières et les atteintes à la réputation peuvent être importantes et si les mesures adéquates n'ont pas été prévues, la conti-

nuité de l'activité peut très rapidement être remise en question. Il est donc primordial d'être bien informé des risques courus par votre entreprise ainsi que des moyens qui peuvent la prémunir contre ces risques afin d'augmenter vos chances de maximiser et de fidéliser votre clientèle.

Depuis le 25 mai 2018, le nouveau règlement européen relatif à la protection des données (« RGPD » ou « GDPR »[1] en anglais) est d'application. Ce règlement impose diverses obligations en matière de protection des données à toutes les entreprises installées dans l'espace européen[2].

Parmi ces nouvelles obligations figure notamment celle de prendre les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel traitées par votre entreprise. Le présent document vous aidera à mieux comprendre ces mesures techniques et organisationnelles et à les intégrer dans votre entreprise.

Le non-respect des dispositions du RGPD (ou GDPR) est sanctionné de lourdes amendes variant selon le type d'infraction mais pouvant atteindre 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu !

Pour en savoir plus, n'hésitez pas à consulter le site de l'Autorité de protection des données ainsi que le point 3.2.4. du présent document : « Principe 4. Prévoyez les dispositions relatives à la protection de la vie privée ».

N'attendez pas la dernière minute pour mettre en place ou développer une politique de protection des données efficace !

Limiter les risques pour votre entreprise, être en conformité avec le RGPD (GDPR), rassurer les partenaires professionnels et disposer d'une bonne e-réputation vis-à-vis des consommateurs demande de développer une stratégie numérique intégrant les mesures de sécurité nécessaires.

Or, seul un faible pourcentage de petites et moyennes entreprises connaissent les obligations qui pèsent sur elles lorsqu'elles disposent d'un site web et/ou qu'elles traitent des données à caractère personnel.

1 Voir Glossaire

2 Art. 3 GDPR. Le GDPR s'applique également aux entreprises situées hors de l'espace européen si les personnes concernées sont européennes (offre de biens, services, ou encore profilage) et/ou si le droit d'un Etat membre s'applique via les règles de droits international public.

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

Parce que notre économie est de plus en plus liée au web, le SPF Economie collabore activement avec la CyberSecurity Coalition et le Centre pour la CyberSécurité Belgique (CCB) pour fournir l'information nécessaire aux entreprises. Dans ce cadre, le présent manuel a pour but de vous fournir les informations nécessaires.

Ces informations se présentent dans l'ordre suivant :

- les mentions obligatoires qui doivent figurer sur votre site internet quel que soit le niveau de maturité de votre entreprise (1.0 ou 2.0) ;
- l'Entreprise 1.0 représente le niveau débutant ou semi-débutant ; (5 principes, 6 actions) ;
- l'Entreprise 2.0 représente le niveau confirmé ou expert (10 principes, 12 actions) ;
- le top 10 des incidents en Europe ;
- en cas d'incident : que faire ?;
- les principaux standards.

Pour vous aider à déterminer le niveau de maturité de votre entreprise en matière de cybersécurité, n'hésitez pas à remplir le questionnaire d'auto-évaluation disponible sur le site web du SPF Economie.

Pour d'autres questionnaires de maturité, vous pouvez également consulter :

- le Guide ICC de la cybersécurité à l'intention des entreprises ;
- l'outil de maturité numérique des PME développé par Digital Wallonia
- l'outil luxembourgeois proposé par CASES concernant l'auto-évaluation des PME qui vous propose, en fonction de votre profil, de suivre la stratégie adaptée votre profil de « start » à « top ».

Vous ne comprenez pas certains termes employés ? N'hésitez pas à consulter notre glossaire.

2. Sites web : nom de domaine et mentions obligatoires

2.1. Nom de domaine

Disposer de son site web demande tout d'abord d'acquérir un nom de domaine.

Comment le choisir ?

- Choisissez un nom de domaine en lien avec votre entreprise, facile à écrire et à mémoriser ;
- Privilégiez une extension connue (.eu ou .be par exemple) ;
- Pensez à réserver des variantes au nom de domaine choisi (cela vous évitera de souffrir des pages concurrentes avec un nom quasiment similaire au vôtre) ainsi que des extensions différentes avec le même nom (.eu ou .brussels si vous avez choisi .be par exemple) afin d'éviter le détournement de trafic ;
- Votre nom sur la toile ne doit pas changer de propriétaire tous les ans : prévoyez si possible de réserver le nom pour la durée maximale autorisée et vérifiez régulièrement les échéances de renouvellement de votre nom de domaine afin d'éviter les mauvaises surprises ;

- N'oubliez pas d'indiquer et de mettre à jour les informations relatives à :
  - » l'identité du titulaire du nom de domaine,
  - » le contact administratif de la base de données WHOIS du registre.
- Si vous pensez sous-traiter la gestion de votre site à un tiers, n'oubliez pas de rédiger un contrat prévoyant qu'à la fin du contrat, le nom de domaine vous soit restitué. N'oubliez pas de prévoir un droit d'accès à vos données durant toute l'exécution du contrat avec votre sous-traitant (identifiants, mots de passes,...).
- Vérifiez régulièrement votre site web, et réagissez rapidement si vous estimez qu'il y a une réservation abusive d'un nom de domaine quasiment semblable au vôtre en recourant aux procédures arbitrales et judiciaires existantes.

Pour plus d'informations

- Pages « noms de domaines » du site web du SPF Economie
- Le guide des bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine de l'Agence nationale des systèmes de sécurité de l'information (ANSSI).

2.2. Mentions obligatoires

Vous disposez d'un nom de domaine mais encore faut-il que les mentions obligatoires figurent sur votre site web !

Si vous êtes constitué en société, les articles 78 et 80 du Code des sociétés énoncent qu'à moins d'engager votre responsabilité personnelle, les mentions suivantes doivent figurer sur tous vos actes y compris sur votre site internet :

1° la dénomination de la société ;

2° la forme, en entier ou en abrégé, (société à responsabilité limitée (SRL), société anonyme (SA), société coopérative (SC), etc.)

- selon le cas, les mots « société civile à forme commerciale » reproduits lisiblement et placés immédiatement avant ou après le nom de la société ;
- dans le cas d'une société coopérative, si elle est à responsabilité limitée ou illimitée ;
- dans le cas de sociétés à finalité sociale, cette mention ou ces initiales doivent être suivies des mots « à finalité sociale » ;

3° l'indication précise du siège (social) de la société ;

4° le numéro d'entreprise (BCE) ;

5° le terme « registre des personnes morales » ou l'abréviation « RPM », suivi de l'indication du siège du tribunal dans le ressort territorial duquel la société a son siège social ;

6° le cas échéant, l'indication que la société est en liquidation.

Si vous exercez une profession réglementée (p. ex., une profession libérale) :

- l'association professionnelle ou l'organisation professionnelle auprès de laquelle vous êtes inscrit ;
- votre titre professionnel et l'Etat dans lequel il a été octroyé ;
- une référence aux règles professionnelles applicables et aux moyens d'y avoir accès.

D'autres dispositions légales peuvent également s'imposer à vous.

- TVA : n'oubliez pas de mentionner votre numéro de TVA.
- Contact : vos coordonnées, y compris votre adresse de courrier électronique, permettant d'entrer en contact rapidement et de communiquer directement et efficacement avec vous.
- Données à caractère personnel : n'oubliez pas d'indiquer les coordonnées de votre délégué à la protection des données (DPO) ainsi que votre « privacy policy[3] » (voir le point 3.2.4 Principe 4. Prévoyez les dispositions relatives à la protection de la vie privée, voir également le site de l'Autorité de protection des données).
- Cookies : l'article 5, §3 de la directive 2002/58/CE a posé le principe d'un consentement préalable de l'utilisateur avant le stockage d'informations sur l'équipement d'un utilisateur ou l'accès à des informations déjà stockées, sauf si ces actions sont strictement nécessaires pour la délivrance d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. Attention : la directive 2002/58 sera prochainement remplacée par un nouveau règlement européen (ePrivacy Regulation) afin d'être conforme au nouveau règlement général sur la protection des données (RGPD).

3 Politique en matière de protection des données à caractère personnel

- Droits d'auteur : vous souhaitez utiliser des œuvres protégées par le droit d'auteur sur votre site, comme par exemple, de la musique, des œuvres audiovisuelles, des articles de presse, des extraits d'œuvre littéraire, etc. ? Savez-vous comment vous y prendre pour ne pas commettre d'infraction à la législation sur le droit d'auteur ? Le SPF Economie répond aux questions les plus fréquentes en la matière.
- Codes de conduite : la mention des codes de conduite auxquels vous êtes éventuellement soumis ainsi que les informations relatives à la façon dont ces codes peuvent être consultés par voie électronique.

Attention : si votre site permet de passer un contrat directement avec un consommateur, certaines dispositions particulières s'appliquent à vous (essentiellement le Livre VI du Code de droit économique pour les sociétés et le livre XIV pour les professions libérales). Pour en savoir plus, n'hésitez pas à consulter la page « Ventes par internet » du site du SPF Economie.

3. Entreprise 1.0

Idéalement, une entreprise 1.0 peut fournir des informations en ligne sur les biens ou services qu'elle propose à l'achat mais ne devrait pas, à ce stade, proposer de paiement en ligne à ses clients ou, si elle le fait, devrait recourir à des services externes de confiance pour assurer la sécurité des transactions.

La grande majorité des entreprises dispose de données importantes (secrets de fabrication, clientèle, facturation, comptabilité...) ainsi que d'outils de travail qui lui sont indispensables. Il est donc primordial pour l'entreprise de protéger ses données et outils de manière adéquate.

Pour atteindre un plus haut degré de maturité en matière de sécurité de l'information, il convient d'agir sur le long terme, en mettant en place un certain nombre d'actions à court et moyen terme.

Afin d'obtenir des premiers résultats à court terme, vous pouvez entreprendre plusieurs actions.

Identifiez les mesures simples et rapides qui permettront de sensibiliser vos employés à la sécurité des outils et à la protection des données de votre entreprise. Ces mesures dépendront naturellement du degré de maturité de votre entreprise mais pour les premiers pas, vous pouvez commencer par :

- cibler les mises à jour du système d'exploitation (OS) et des applications (softwares) ;
- conditionner l'accès au wi-fi de l'entreprise (via un code d'accès) ;

- appliquer une véritable politique de gestion des mots de passe de vos employés ;
- prévoir une gestion des back-up des données vitales à votre entreprise, etc.

Pour vous aider à faire vos premiers pas en cybersécurité , voici 5 principes clefs et 6 actions faciles à mettre en place au sein de votre entreprise.

Pour en savoir plus sur ces principes et actions, n'hésitez pas à consulter le site web de la Chambre de commerce internationale (ICC) et le guide ICC de la cybersécurité à l'intention des entreprises.

3.1. 5 principes clefs en matière de sécurité

3.1.1. Principe 1. Concentrez-vous sur l'information, pas sur la technologie

Il n'y a que 24 heures dans une journée et votre core business n'est pas de faire de la cybersécurité ? Alors concentrez-vous sur l'essentiel en vous focalisant sur la protection de vos informations vitales et construisez pas à pas votre entreprise de demain.

Tout n'est pas qu'une question d'outils technologiques, vos employés peuvent aussi devenir une solide barrière de sécurité ! De nombreux incidents sont dus à une erreur humaine[4], et de très nombreuses attaques auraient pu échouer si l'entreprise avait formé ses employés à traiter l'information de manière plus sécurisée.

Pensez notamment à les sensibiliser aux risques comme le phishing (ingénierie sociale).

Pour vous y aider, vous pourrez trouver une campagne de sensibilisation des employés concernant le phishing sur le site web de la Cybersecurity Coalition.

Votre entreprise conçoit un nouveau programme ? Vous faites l'inventaire des informations dont vous disposez ? Pensez à envisager votre approche de manière globale. Si vous concevez la sécurité de l'information et la protection des données à caractère personnel dès le début, vous gagnerez un temps précieux dans la réalisation de votre projet ! A défaut, vous devrez peut-être tout recommencer avant de le voir aboutir ou payer plus cher pour corriger les défauts d'un programme.

Si vous innovez, pensez immédiatement « sécurité » et « vie privée ».

4 Voir notamment le point « Top 10 des incidents ».

3.1.2. Principe 2. Instaurez une attitude de résilience : apprenez à rebondir plus facilement

De nombreuses législations s'appliquent aux entreprises mais « être en conformité » avec ces obligations légales ne signifie pas forcément que votre entreprise est correctement protégée face aux risques cyber. Pensez au-delà de vos obligations légales strictes et prévoyez une défense adaptée à vos besoins.

Si vous connaissez les règles qui s'appliquent à vous et si vous pensez à limiter vos risques, vous serez en mesure de rebondir plus facilement après un incident.

3.1.3. Principe 3. Préparez-vous à réagir

Sur le web, il n'est pas question de savoir si vous serez frappé un jour mais uniquement de savoir QUAND vous le serez. Préparez-vous donc à réagir au mieux !

Pensez notamment à vérifier si :

- vous savez qui contacter pour régler les problèmes techniques ;
- vous savez où se trouvent vos back-up et comment y accéder rapidement ;
- vous savez quelles autorités compétentes avertir et comment les avertir ;
- vous êtes couverts ou non par une assurance et si oui, quels dommages sont couverts par votre cyberassurance ;
- vous avez pensé à une stratégie de communication envers vos partenaires professionnels (fournisseurs, etc.) et envers vos clients…
- vous avez pris le temps de faire partie d'une communauté de vos pairs (comme, par exemple, la CyberSecurity Coalition) afin d'être avertis des tendances actuelles concernant les cybermenaces qui pèsent sur votre secteur, votre type d'entreprise, etc.

3.1.4. Principe 4. Montrez que vous prenez vos responsabilités

Trop « petit » et donc « pas concerné » ? Rien n'est plus faux ! Les PME représentent une cible de choix pour les hackers car elles constituent une grande partie du tissu économique national, elles disposent d'un grand nombre d'informations (données de leurs clients, savoir-faire, secrets d'affaires…) et elles peuvent également servir de point d'entrée pour atteindre de plus grosses cibles avec lesquelles les PME sont en relation de confiance (fournisseurs, etc.).

« Je ne me suis jamais fait voler, cela n'arrive qu'aux autres »..Mais votre entreprise pourrait-elle détecter une intrusion ? Pourquoi le hacker vous ferait-il savoir qu'il dispose de ses entrées chez vous et chez vos clients ?

De nouvelles sanctions peuvent frapper l'entreprise en cas d'infraction aux règles fixées par le règlement européen de la protection des données (RGPD/GDPR) : jusqu'à 20 millions d'euros[5] ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Si la Direction se sent concernée et s'implique en montrant le bon exemple, les employés comprendront qu'il est important, pour eux aussi, de s'investir.

Comment montrer que vous prenez vos responsabilités ?

- Pensez à désigner un point de contact en cas d'incident

Le « point de contact » peut être interne ou externe. Selon la taille et les besoins de votre entreprise, cette fonction pourrait même être accomplie à temps partiel (attention toutefois à éviter les éventuels conflits d'intérêt) ou assumée par un groupe de personnes.

Attention ! Le « point de contact » ne devient pas responsable de tout ! Il a pour fonction de faire remonter l'information au bon niveau de pouvoir afin de permettre à votre entreprise de réagir vite et efficacement en cas d'incident. Chaque employé reste responsable de ses actes et l'employeur doit veiller à sensibiliser et à responsabiliser l'ensemble de son personnel.

- Prévoyez un moyen de contrôler le respect de votre politique de sécurité

Prévoyez des tests et des audits concernant la sécurité de l'information et n'oubliez de demander des rapports réguliers (à chaque incident, tous les mois...)

  - » sur l'efficacité et la pertinence des mesures techniques et organisationnelles mises en place au sein de votre entreprise
  - » sur les pistes d'amélioration qui pourraient être suivies.

Pour un premier pas, l'audit peut être simple et ne porter que sur une partie de votre système d'information, l'objectif est d'identifier les pistes d'amélioration (quick-wins) qui pourraient être envisagées par votre entreprise. A ce stade, l'idéal serait d'investir davantage dans la protection de votre système d'information et non de payer des audits fort avancés qui n'auraient pas beaucoup de sens pour une entreprise 1.0.

5 Pour en savoir plus, consultez le point « Entreprise 2.0, Principe 4 Prévoyez les dispositions relatives à la protection de la vie privée ».

- Osez-vous remettre en question

  Les menaces ne sont pas figées une bonne fois pour toutes. Vos vulnérabilités non plus. Pensez plutôt à une amélioration constante de votre gestion des risques et osez revoir votre politique de sécurité régulièrement (tous les ans). Tout ne devra pas changer mais certains points pourraient sûrement être améliorés.

3.1.5. Principe 5. Mettez votre vision en œuvre

- Adoptez une bonne politique de sécurité de l'information

Une politique de sécurité de l'information rend visible votre volonté de protéger vos atouts les plus importants (informations, réputation...) et permet d'offrir à tous vos employés un cadre de référence leur expliquant ce qu'ils peuvent/ne peuvent pas faire en matière de sécurité de l'information.

- Pensez à vos relations externes

a) Avec vos fournisseurs numériques

Interrogez vos fournisseurs de services numériques : ils peuvent, le plus souvent, vous proposer des solutions de sécurité. Ces solutions de sécurité peuvent notamment comprendre :

- la gestion des back up (sauvegardes),
- la gestion de points de restauration (recovery)[6],
- la cryptographie[7],
- des audits de votre système de sécurité de l'information,
- la mise à disposition d'un cloud privé, etc.

Pensez également à demander de pouvoir accéder aux traces d'activités (logs) pour les services que vous avez externalisés. En cas d'incident, ces traces seront essentielles pour savoir ce qui s'est passé et pour éviter qu'un incident du même type se reproduise à nouveau.

b) Avec vos autres fournisseurs

Assurez-vous que vos fournisseurs disposent eux aussi d'une politique de sécurité de l'information suivie d'effets. Leurs incidents de cybersécurité peuvent également affecter vos opérations commerciales et/ou votre réputation. N'hésitez pas à deman-

6 Voir Glossaire.

7 Voir Glossaire.

der s'ils disposent d'une certification (voir point 8. Principaux standards), et demandez à recevoir une copie des audits de sécurité (minimum une fois par an)...

c) Avec vos partenaires professionnels

Pensez à discuter de la sécurité de l'information en tant que chaîne complète avec vos partenaires professionnels. Certes, vous aurez fait le maximum de votre côté pour assurer votre sécurité mais eux aussi ont tout intérêt à se protéger ! A défaut, vos partenaires professionnels pourraient servir de porte d'entrée pour infecter vos systèmes et pourraient également ne plus être capables de répondre à vos besoins, par exemple en raison d'une cyber-attaque qui paralyserait leur chaine de production.

Ne pensez pas tout faire tout de suite : dressez une feuille de route des points d'action à entreprendre en priorité en tenant compte de vos véritables besoins et des moyens budgétaires et humains dont vous disposez.

Vous ne comprenez pas certains termes employés ? N'hésitez pas à consulter notre glossaire.

3.2. 6 Actions

3.2.1. Action 1. Sauvegardez vos informations et validez le processus de récupération

Que se passerait-il si tous vos ordinateurs se trouvaient infectés en dix minutes ? Disposez-vous d'une copie de vos informations vitales ? Cette copie est-elle reliée par réseau aux ordinateurs infectés ? Etes-vous sûr que vos copies sont valables et qu'elles ne seront pas infectées elles aussi ? Avez-vous choisi un service de cloud et si oui, quelles sont les garanties offertes en matière de confidentialité, d'intégrité et d'authenticité ?

Pensez à vous poser les bonnes questions avant...pour éviter bien des ennuis en cas d'incident.

Sauvegarder vos informations de manière efficace implique :

a. que vous puissiez identifier quelles informations il vous faut conserver (classez vos informations) ;
b. que vous mettiez en place des procédures de sauvegarde (back up) ;
c. que vous fassiez régulièrement des tests afin de vérifier la qualité de vos sauvegardes ainsi que des processus de récupération.

a) Classez vos informations

Un simple e-mail d'information générale à destination de l'un de vos clients ne se protège pas de la même façon qu'une invention de votre entreprise. Pensez à identifier les informations vitales de votre entreprise pour mieux les protéger.

Voici un exemple de modèle de classification simple à suivre :

« Publics » : Tout le monde devrait pouvoir accéder à ces informations aussi bien au sein de votre entreprise qu'à l'extérieur. Ces informations n'exigent pas de protection, de marquage ni de traitement particuliers. Les actualités ou le numéro de contact général que vous affichez sur le site web de votre entreprise sont un bon exemple d'information pouvant être labellisées « publics » ;

« Restreints » : Seules certaines personnes déterminées devraient pouvoir accéder à ces informations. Les personnes pouvant y avoir accès sont généralement limitées à un groupe choisi de personnes, dont certains employés, clients, fournisseurs... Ces renseignements devraient être contrôlés par diverses mesures de protection et devraient être étiquetés « restreints ». Le règlement de travail de votre entreprise ou les numéros de contact professionnels de tous vos employés sont un bon exemple de renseignements restreints ;

« Confidentiels » : L'accès à ces renseignements n'est autorisé qu'à un nombre restreint de personnes désignées au sein de votre entreprise. La perte ou le vol de ces renseignements pourrait nuire gravement à votre entreprise. Les documents ou renseignements « confidentiels » doivent être étiquetés et traités avec précaution et ne devraient idéalement pas sortir de votre entreprise. Les éléments de votre entreprise couverts par le secret des affaires ainsi que les données à caractère personnel sur vos clients sont des exemples de renseignements confidentiels.

N'oubliez pas de consigner par écrit les règles applicables à l'étiquetage, au traitement ou à la transmission des informations et documents et de former vos employés au respect de ces règles.

b) Mettez en place des procédures de sauvegarde

Tout ne doit pas forcément être sauvegardé. Identifiez l'information dont vous avez besoin et imaginez-vous la perdre demain. De quoi auriez-vous besoin pour rebondir rapidement ? Sous quel format l'information vitale serait-elle plus vite récupérée ?

Pensez également :

- si possible, à sauvegarder ces informations dans un lieu autre que vos locaux principaux (risques d'incendie, d'inondation…)
- si besoin, à externaliser (cloud) : dans ce cas, pensez à exiger un bon niveau de sécurité, la possibilité d'organiser des audits externes, des tests de récupération, et, pourquoi pas, cryptez vos données stockées…
- à séparer vos environnements : si votre PC (ordinateur) est infecté par un ransomware, vos sauvegardes seraient-elles touchées également ?

c) Organisez des tests réguliers

N'oubliez pas d'organiser des tests afin de vérifier la qualité de vos sauvegardes (avez-vous bien récupéré toute l'information stockée ?) ainsi que la qualité de vos processus de sauvegarde (a-t-il été facile de récupérer ces données ? avez-vous détecté des conflits logiciels ?, etc.).

3.2.2. Action 2. Mettez à jour vos systèmes informatiques

De nouvelles vulnérabilités sont régulièrement découvertes. Une fois les vulnérabilités identifiées, les programmes officiels mettent tout en œuvre pour combler ces failles grâce à des « patches ». Encore faut-il que vous mettiez régulièrement à jour votre système d'exploitation (OS) et vos softwares (logiciels) afin qu'ils disposent des derniers patches disponibles ! Pensez à mettre régulièrement à jour tous vos programmes. Les mises à jour automatiques des programmes antimalwares, des outils de filtrage web, des systèmes de prévention d'intrusion (IPS[8]) et des systèmes de détection d'intrusion (IDS[9]) sont à recommander.

3.2.3. Action 3. Investissez dans la formation

La sécurité est l'affaire de tous ! N'oubliez pas d'en parler régulièrement à vos employés, de les former et de les informer sur les bonnes pratiques en usage dans votre entreprise et, pourquoi pas, de solliciter l'avis de vos employés sur les vulnérabilités de votre entreprise et/ou sur les bons moyens de les diminuer sensiblement.

La formation peut être interne et/ou externe, ce qui compte c'est d'instaurer une nouvelle culture de sécurité des données au sein de l'entreprise.

8 Voir Glossaire.

9 Voir Glossaire.

3.2.4. Action 4. Surveillez votre environnement informatique

- Accès et équipements

Déterminez qui peut accéder à vos ordinateurs, votre réseau ! Un fournisseur peut-il y accéder ? Avez-vous protégé votre environnement (bâtiments, serveurs…)? Si vous ne disposez pas des compétences nécessaires, pensez à externaliser (cloud) [10].

Déterminez quels équipements (appareils mobiles…) peuvent être autorisés à accéder au réseau/aux informations de votre entreprise et pensez à sécuriser vos appareils (mots de passe, cryptographie, blocage à distance…).

Un ordinateur portable, une tablette, un GSM, une clef USB ? Ces objets se perdent… ou se volent rapidement ! En cas de perte ou de vol, des tiers pourraient accéder à des informations précieuses si vous n'avez pas pensé à crypter (chiffrer) vos données ou si vous n'avez pas physiquement interdit l'utilisation de certains supports (par exemple, vous pourriez obturer les ports USB sur les PC de l'entreprise).

Pensez également à indiquer à vos employés comment vous avertir rapidement en cas d'incident (par exemple : si un appareil mobile contenant des données de votre entreprise a été volé ou perdu).

- Mot de passe

Un mot de passe, c'est comme une brosse à dents ! Faites comprendre à vos employés qu'un mot de passe ne se prête pas et que le mot de passe de l'entreprise ne devrait pas être utilisé à d'autres fins (Facebook, messagerie personnelle, sites de rencontre…).

Obligez chaque employé à recourir à un mot de passe suffisamment long (minimum 8 caractères) incluant au moins une majuscule, des minuscules, des chiffres, un caractère spécial (ex. : (!,%,@)…)

Pensez à demander un renouvellement des mots de passe régulier (idéalement au moins une fois par saison) et à faire en sorte qu'un même mot de passe ne puisse pas éternellement être réemployé.

Insistez pour que les mots de passe choisis ne soient pas reproduits sur des supports bien en vue dans le bureau (post it, tableau…) et évitez les pièges de débutant en refusant les mots de passe les plus courants : 1234567 (17 % des utilisateurs !), 123456789, motdepasse, password, google, azertyuiop, qwerty, qwertyuiop, mynoob, 123qwe, 123azer…

Ces « mots de passe » sont si faciles à introduire que cela revient à laisser vos clefs sur la porte de votre entreprise !

10 Dans ce cas, voir Entreprise 2.0, « Principe 10. Prévoyez les relations avec les tiers ».

Pour les accès à distance (télétravail, réunion à l'extérieur…), ne vous reposez pas que sur un mot de passe et privilégiez une approche prenant en compte au moins deux facteurs (par exemple : mot de passe + recours à la carte d'identité via CSAM). Pensez également à ne pas confier des informations sensibles via une connexion publique (wi-fi public) et à privilégier une connexion sécurisée (en passant par un VPN[11]).

Si vous voulez en savoir plus sur les mots de passe, consultez les recommandations de l'ANSSI et de la CNIL (France).

Vous voulez savoir si votre mot de passe est suffisamment fort ? Vous pouvez le tester au préalable.

Vos employés se plaignent de devoir utiliser plusieurs mots de passe et/ou de régulièrement les oublier ? Utiliser un gestionnaire de mots de passe comme Keepass ou Zenyway par exemple.

- Règles de bon sens

Pensez à rappeler des règles de prudence à vos employés :

» ne « chattez » pas avec des inconnus sur le réseau de l'entreprise ;

» ne donnez aucune information bancaire par e-mail ou par téléphone sans avoir vérifié l'identité de cette personne de plusieurs manières ;

» regardez dans le coin supérieur gauche de votre écran et vérifiez si l'adresse web mentionnée est sécurisée c'est-à-dire qu'elle commence par un https:// (avec l'icône d'un cadenas fermé);

» vérifiez si le site sur lequel on vous envoie ne comporte pas de faute d'orthographe dans le nom et contient une section « contact » et une section « protection de la vie privée ». Vérifiez également si les autres mentions obligatoires figurent bien sur le site web de votre correspondant.

Limitez les comptes administrateurs [12]

- Tous vos employés peuvent-ils installer n'importe quel programme sur leur ordinateur ? Comment saurez-vous si votre entreprise respecte les conditions générales des licences (programmes) qu'elle a acquises si chacun peut mettre n'importe quoi sur son PC ? Assurez-vous que seul un petit nombre d'administrateurs IT disposent des droits d'accès sur vos ordinateurs. Ne vous reposez pas non plus sur une seule personne et pensez à prévoir un monitoring régulier des comptes administrateurs car ces derniers représentent une cible de choix pour les hackers.

11 Voir Glossaire.

12 Voir Glossaire.

3.2.5. Action 5. Multipliez les lignes de défense pour réduire les risques

Il existe de nombreux malwares[13] et chaque jour de nouveaux programmes nuisibles voient le jour.

Pensez à disposer au minimum :

- d'un antivirus ;
- d'un firewall[14] (pare-feu) ;
- de programmes de prévention d'intrusion et de détection d'intrusion (IPS/IDS[15]) ;
- pensez à mettre ces programmes à jour régulièrement (/automatiquement).

N'oubliez pas non plus de prévoir :

- une bonne politique de sécurité de l'information ;
- une bonne formation de vos employés.

Enfin, n'hésitez pas à contracter une cyberassurance si besoin.

3.2.6. Action 6. Préparez-vous à faire face aux incidents

Avez-vous tout prévu en cas d'incident ?

Savez-vous :

- détecter un incident ?
- qui contacter pour prendre des décisions ?
- quelles autorités contacter ?
- qui peut vous aider techniquement ? (sauvegardes,...)
- quelles traces (preuves) conserver[16] ?
- comment communiquer envers vos clients/vos partenaires professionnels ?

Pensez à vous préparer maintenant pour éviter bien des dégâts pendant et après un incident.

13 Voir Glossaire.

14 Voir Glossaire.

15 Voir Glossaire.

16 Des lignes directrices sur les données à conserver sont disponibles sur le site web du CERT.eu. Un guide sur les techniques forensic est également disponible sur le site web du NIST.

4. Entreprise 2.0

Si vous désirez que votre entreprise aille plus loin, voici 10 principes et 12 actions qui pourront utilement être mis en place au sein de votre entreprise.

4.1. Etape 1. Analyse de risques ou « Connaissez-vous vous-même » !

La première étape consiste à réaliser une analyse de risques. Il s'agit d'une démarche qui vous permettra d'identifier rapidement quels sont vos actifs critiques afin de les protéger au mieux. L'analyse de risques peut être :

a) rudimentaire, sur la base de simples questions

- Votre entreprise dispose-t-elle d'une politique de sécurité de l'information ? (Oui/Non)
- Planifiez-vous de développer et/ou de mettre à jour une politique de sécurité de l'information et/ou une politique de protection des données à caractère personnel endéans les 12 prochains mois ? (Oui/Non)
- Si la réponse à l'une des deux premières questions a été non, quelle en est la raison principale ? (manque d'expertise, trop onéreux, pas assez de personnel…)

- Avez-vous développé ou souhaitez-vous implémenter des standards[17] en matière de sécurité et/ou de protection de données à caractère personnel ? (Oui/Non)
- Votre politique de sécurité a-t-elle prévu les éléments suivants :
  - » Relation avec les membres du personnel (règlement de travail, clauses de confidentialité...)
  - » Gestion des risques (y compris audit régulier, rapport...)
  - » Politique en matière de protection de données à caractère personnel (registre adéquat, informations à fournir aux autorités, aux personnes concernées...)
  - » Business Continuity Plan (BCP)[18] (Plan de continuité des activités d'entreprise)
  - » Disaster Recovery Plan (DRP)[19] (plan de continuité après un désastre)
  - » Crisis Management Plan (CMP) (plan de gestion de crise)
  - » Governance, Risk management and Compliance (GRC) (gestion des processus, des risques et de vos obligations légales et contractuelles)
  - » Incident Management Plan (plan de gestion des incidents)
  - » Journal de suivi des incidents
  - » Relations avec les tiers (contrats de services, de livraison, clauses à prévoir en matière de sécurité et de confidentialité, consultants se trouvant régulièrement dans vos locaux...)
  - » Un point particulier pour chacun des incidents les plus fréquents[20]
- Au bout de combien de temps sans accès à internet commenceriez-vous à avoir des problèmes pour gérer votre entreprise (quelques minutes, quelques heures, quelques jours) ? Qu'est-ce qui vous gênerait en premier ?
- Que se passerait-il si l'un de vos concurrents devait découvrir les informations dont vous disposez (liste de clients, secrets de fabrication, fournisseurs particuliers...) ?

Le site web du SPF Economie vous propose un questionnaire d'évaluation pour vous aider.

17 Voir le point « Principaux standards »

18 Voir Glossaire.

19 Voir Glossaire.

20 Voir le point « Top 10 des incidents».

Pour d'autres questionnaires de maturité, vous pouvez également consulter

- le Guide ICC de la cybersécurité à l'intention des entreprises,
- l'outil de maturité numérique de DigitalWallonia ou
- le site luxembourgeois CASES avec l'auto-évaluation des PME qui vous propose, en fonction de votre profil, différentes stratégies de « start » à « top ».

b) plus complexe en ayant recours à des méthodologies et outils spécifiques :

- MEHARI
- EBIOS,
- MONARC,
- OCTAVE
- CRAMM
- ...

Pour en savoir plus sur les différentes méthodologies d'analyse de risques, vous pouvez consulter le site de l'European Network and Information Security Agency ENISA

Qu'elle soit rudimentaire ou complexe, l'analyse de risques part du principe que le risque est le résultat que la probabilité d'une menace (intérieure ou extérieure) exploite une vulnérabilité de votre entreprise et vous inflige un dommage (impact).

Si le dommage (l'impact) est considéré comme négligeable, la direction peut considérer le risque comme « acceptable ». Elle doit cependant clairement identifier ce qu'elle considère comme « acceptable » ou non.

Pour calculer le risque, on multiplie la probabilité d'une menace par la vulnérabilité et l'impact ce qui peut se résumer suivant la formule suivante :

Risque = (Probabilité . Menace) . Vulnérabilité . Impact

Il est difficile d'agir sur les menaces car ces dernières évoluent sans cesse.

Toutefois, il est possible de diminuer les risques en agissant sur les autres points de l'équation.

Il est ainsi possible de diminuer le risque qu'une menace exploite vos vulnérabilités en diminuant vos vulnérabilités. Par exemple, sans aucun antivirus, la probabilité qu'un virus frappe votre entreprise et commette de graves dommages est évidemment plus grande que si vous aviez mis en place une protection à plusieurs niveaux comprenant, notamment, un antivirus régulièrement mis à jour.

Il est également possible de diminuer vos dommages (impact) en diminuant les risques jusqu'à un niveau de risque acceptable et/ou en mitigeant[21] c'est-à-dire en limitant et/ou en transférant tout ou partie de vos risques. Par exemple, si un ransomware[22] frappe l'un des ordinateurs de votre entreprise mais que vous disposez d'une bonne gestion de vos copies de sauvegarde (back-up) et que tout le monde sait comment réagir grâce aux mesures de sensibilisation de votre entreprise, cet incident pourra rapidement être résolu et votre entreprise pourra fonctionner normalement au bout de quelques minutes.

Depuis le 25 mai 2018, le nouveau règlement général sur la protection des données («RGPD/GDPR[23] ») est d'application. Ce nouveau règlement impose diverses obligations en matière de protection de la vie privée parmi lesquelles celle de prendre les mesures techniques et organisationnelles appropriées pour assurer la protection des données à caractère personnel traitées par votre entreprise[24] et, dans certains cas, l'obligation de réaliser une analyse d'impact relative à la protection des données (« Data Protection Impact Assessment » dit « DPIA »[25]).

Les sanctions prévues par le GDPR[26] peuvent aller, en fonction du type d'infractions, jusqu'à :

- 10.000.000 d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu ;
- 20.000.000 d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Toutefois, les risques d'encourir une telle amende diminuent fortement si vous avez fourni l'information nécessaire aux personnes concernées et si vous avez implémenté les mesures techniques et organisationnelles appropriées. Autant prévoir dès le début dans votre analyse de risques ainsi que dans votre politique de sécurité de l'information l'angle relatif à la protection de la vie privée !

Même si l'objectif principal du GDPR (RGPD) n'est pas d'éviter les cyberattaques, il n'en est pas moins vrai qu'en respectant ce nouveau règlement et les mesures techniques et organisationnelles qu'il impose vous limiterez fortement les effets néfastes de la plupart des cyber-attaques ! Non seulement vous respecterez les obligations

21 Voir Glossaire.

22 Voir Glossaire

23 Voir Glossaire.

24 Art. 32 RGPD.

25 Voir art. 35 et suivants RGPD.

26 Art. 83 RGPD.

légales qui pèsent sur votre entreprise mais vous pourrez également profiter de cette opportunité pour faire savoir à vos clients personnes physiques à quel point vous prenez le respect de leur vie privée au sérieux !

Afin d'en savoir plus sur ces matières, nous vous conseillons de visiter le site de l'Autorité de protection des données et de vous tenir au courant des guidelines fournies par le Comité européen de protection des données[27] (ancien « groupe de travail article 29 »).

Pour en savoir plus sur les mesures que vous pouvez mettre en place afin de diminuer l'impact et/ou les vulnérabilités, consultez le point « Top 10 des incidents ».

Pensez également à consulter le point « Principe 4. Prévoyez les dispositions en matière de protection de la vie privée ».

Ne pensez pas tout faire tout de suite : dressez une liste des risques les plus élevés en tenant compte de vos véritables besoins et des moyens budgétaires et humains dont vous disposez. Les risques qui sont fort probables et qui peuvent entrainer de graves dommages (impacts) devraient être traités en priorité.

Pour en savoir plus, consultez le Guide « Data Protection » publié par la FEB (Fédération des Entreprises de Belgique) ainsi que le site web de la Cybersecurity Coalition.

4.2. Etape 2. 10 principes

4.2.1. Principe 1. Adoptez une défense « multi-couche »

Dans une boîte à outils, chaque outil a sa fonction. Il en va de même pour les aspects cyber : prévoyez une défense qui ne repose pas sur un seul outil ! Pensez à disposer notamment des outils suivants :

- antivirus ;
- firewall (pare-feu) ;
- softwares (logiciels) anti-spam[28], anti-phishing[29], anti-exploit, anti-ransomwares[30], anti-malwares[31]...

27 Art. 68 du RGPD. Voir également le Glossaire.

28 Voir Glossaire.

29 Voir Glossaire.

30 Voir Glossaire.

31 Voir Glossaire.

N'oubliez pas de prévoir des outils vous permettant de détecter des incidents (IDS/IPS)[32] et ne vous reposez pas uniquement sur eux. Enfin, ne perdez pas de vue que la qualité des règles de détection et de corrélation, la couverture des types d'incidents et les processus de réponse en cas de détection doivent également être implémentés de manière efficace.

Votre attention devrait au moins porter sur les éléments de contrôle suivants :

1. gestion des mises à jour de vos outils et des applications (Java, Flash...) ;
2. inventaire des hardwares et softwares autorisés/non autorisés ;
3. configuration efficace (et mises à jour) des éléments hardware et software pour les serveurs, laptops, GSM ;
4. configuration efficace des routers[33], firewalls[34] (pare-feu), switches[35] ;
5. respect des licences des programmes acquis ;
6. analyse régulière des vulnérabilités et des solutions/résolutions possibles ;
7. anti-malwares efficaces ;
8. politique spécifique pour les appareils mobiles ;
9. politique spécifique pour les accès wi-fi et les accès à distance ;
10. scans de tous les mails entrants[36] ;
11. administrateurs (privilégiés) peu nombreux et aux accès nécessaires (+ contrôle spécifique) ;
12. tests réguliers des copies de sauvegarde (back up : qualité et processus) ;
13. plans adaptés : Business Continuity plan, Disaster Recovery Plan, Incident management plan, Crisis management plan...

Pour en savoir plus, consultez le livre blanc du CERT.eu : Mitigating Risks Related to Network Devices (2017)

32 Voir Glossaire.

33 Voir Glossaire.

34 Voir Glossaire.

35 Voir Glossaire.

36 Voir également le livre blanc du CERT.eu « Defeating E-mail Abuse » (2017).

4.2.2. Principe 2. Sensibilisez votre personnel à la sécurité de l'information

Les données dont vous disposez (secret d'affaires, de fabrication, données à caractère personnel...) doivent être correctement protégées[37].

Pour ce faire, vous devez faire savoir à vos employés ce qu'ils peuvent/ne peuvent pas faire des données de l'entreprise en établissant une politique de sécurité efficace accompagnée ou non d'un code de conduite. Ces documents sont à établir, de préférence, en annexe au règlement de travail de votre entreprise.

Afin de gérer vos projets en adéquation avec votre politique de sécurité, l'idéal est de faire appel à des méthodologies éprouvées dans des référentiels tels que :

- ITIL qui propose un ensemble de bonnes pratiques pour assurer un management efficace du système d'information ;
- COBIT qui propose des bonnes pratiques de gouvernance informatique dans une logique de contrôle des risques et de management ;
- Prince2 qui propose une méthode de management de projet axée sur la gestion de projets.

Vous pouvez également vous référez à des standards internationaux tels que la famille des ISO/IEC 27000, la famille des ISO/IEC 9000, les NIST (SP800, SP1800,.) Pour en savoir plus, voir le point 8 « Principaux standards».

Une fois la politique de sécurité et le code de conduite dressés, n'oubliez pas de les faire connaître ! Formez vos employés à bien réagir en appliquant les règles que vous aurez fixées.

Pour sensibiliser votre personnel, pensez à multiplier les canaux d'information : séance d'information à vos nouveaux employés, rappels réguliers dans vos messages internes (newsletter...), sensibilisation des supérieurs hiérarchiques afin qu'ils intègrent le respect de la politique et des règles à suivre dans l'évaluation des employés, soutien à des campagnes de sensibilisation (Safer Internet Day, Take Back the Internet...).

Pour vous aider, voici quelques documents de référence :

- Kit à l'attention des PME : ingéniérie sociale, mots de passe et phishing
- Phishing
- Fraude CEO

37 Voir le point « Principe 4. Prévoyez les dispositions en matière de protection de la vie privée ».

N'oubliez pas que vos employés ramènent les habitudes qu'ils ont acquises à la maison...sur leur lieu de travail !

Pensez à leur donner les informations nécessaires pour que leur comportement sur internet soit plus sûr...où qu'ils soient : cybersimple, info-risques, safeonweb, CCB, Autorité de protection des données... (voir En savoir plus ? Acteurs et liens utiles)

Enfin, pensez à former de manière continue les employés et/ou équipes en charge de la sécurité de l'information et/ou désignés comme point de contact IT. Les menaces changent sans cesse et il vaut mieux se tenir au courant des bonnes pratiques que votre secteur a mises en place.

4.2.3. Principe 3. Identifiez les informations dont dispose votre entreprise et classifiez-les !

Pensez à former votre personnel quant à la classification des documents en interne ! Il s'agit de permettre à chacun de savoir quelles règles s'appliquent pour quel type de données.

Avant de pouvoir « classifier », la première démarche consiste à identifier et à répertorier les informations nécessitant des mesures de protection.

Vous pourriez, par exemple, identifier les informations suivantes :

- techniques : idées originales, connaissance des vulnérabilités d'un produit, savoir-faire particulier, architecture de votre entreprise, designs originaux, plus-value sur un produit ou un service, méthodes de conception, prototypes...
- commerciales : fichiers clients, fichiers fournisseurs, plans marketing, préférences des clients en fonction de divers profils...
- financières : détail des différents postes comptables, contenus et conditions des contrats et offres commerciales, prix d'achat et de vente, assurances...
- stratégiques : projet de recrutement (RH), veille juridique et veille technologique adaptée à votre entreprise, projet d'acquisition/de fusion...

Pensez à impliquer les différents services de votre entreprise : juridique, RH, commercial, informatique, comptabilité...

Une fois l'information identifiée, pensez à la classifier ! Pour ce faire, vous pouvez notamment avoir recours à une classification de type « Traffic Light Protocol » (ou TLP)[38].

38 Voir le document TLP sur le site web du SPF Economie.

Attention, tout n'a pas vocation à être « confidentiel » : agissez avec discernement si vous ne voulez pas décrédibiliser votre démarche. Ainsi, si vous « classifiez » toutes vos informations en TLP Rouge, nombreux seront vos employés, vos clients, vos fournisseurs etc. qui ne pourront jamais avoir accès à l'information que vous auriez pourtant aimé leur communiquer. Assurez-vous que les codes sont réellement attribués en fonction des besoins de votre entreprise et n'oubliez pas de faire en sorte que les lignes hiérarchiques puissent obtenir l'information nécessaire.

Pour en savoir plus sur la classification des informations, vous pouvez également consulter :

La classification (voir point 3.2.1).

Pensez également à partager de manière sécurisée l'information concernant les menaces et les incidents auxquels vous pouvez faire face dans un cercle de confiance formé, idéalement, de pairs de votre secteur d'activité. Ceci vous permettra de prendre rapidement conscience des principales menaces vous concernant mais également d'identifier les solutions qui peuvent être apportées à ces menaces/incidents. Pour un exemple de cercles de confiance, voir notamment la CyberSecurity Coalition et l'European Cyber Security Organization (ECSO).

Partager des informations dans un cercle de confiance implique notamment que vous ayez identifié :

- qui peut partager l'information ;
- quelles informations peuvent être partagées et quelles informations ne peuvent pas faire l'objet d'un tel partage.

4.2.4. Principe 4. Prévoyez les dispositions en matière de protection de la vie privée

NB : le présent point n'a pas pour but de présenter le GDPR/RGPD de manière exhaustive mais simplement d'identifier certains points d'attention. Pour en savoir plus, consultez régulièrement le site de l'Autorité de protection des données.

Le règlement général sur la protection des données (RGPD ou GDPR)[39] impose plusieurs obligations au responsable du traitement (et à son éventuel représentant) ainsi qu'au sous-traitant[40].

39 Voir Glossaire.

40 Voir notamment chapitre IV du RGPD, articles 24 et suivants.

Voici quelques points d'attention à prendre en compte afin de répondre au mieux à ces obligations :

Identifiez les rôles

Afin d'éviter des discussions de dernière minute, pensez à identifier clairement dans vos contrats :

- si vous êtes responsable du traitement :

  les limites que vous entendez fixer à votre sous-traitant, les conventions particulières (convention de confidentialité, audit possible, niveaux de service attendus...).

- si vous êtes sous-traitant :

  les limites que vous impose le responsable du traitement. Vous ne pourrez pas agir en dehors de ces limites.

N'oubliez pas d'avertir le responsable du traitement de tout acte ou directive qui vous paraitrait contraire aux obligations prévues par le GDPR/RGPD.

Attention : le responsable du traitement et le sous-traitant peuvent être condamnés de manière solidaire (art. 82 et 83 du GDPR/RGPD).

Il importe donc que les entreprises fixent les règles qu'elles entendent faire prévaloir dans leur contrat.

Tenez le registre adéquat

D'après le nouveau règlement européen en matière de protection de la vie privée (GDPR/RGPD),

- chaque responsable du traitement (et, le cas échéant, son représentant) doit tenir un registre des activités de traitement. Ce registre doit contenir les informations exigées par l'article 30 GDPR.
- chaque sous-traitant et, le cas échéant, le représentant du sous-traitant tient un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement. Ce registre doit contenir les informations exigées par l'article 30 GDPR.

Consultez l'exemple de registre sur le site web du SPF Economie.

Désignez un délégué à la protection des données[41] (Data Protection Officer ou « DPO ») et pensez à définir les contours exacts de sa fonction ainsi que de ses missions.[42]

Le DPO devrait être désigné sur la base de ses qualités professionnelles et en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, de sa bonne connaissance de votre entreprise et de sa capacité à accomplir les missions que vous lui aurez confiées. N'oubliez pas de faire passer le message auprès de vos différents services : le DPO doit être associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel.

S'il s'agit d'un DPO interne, veillez à le faire dépendre directement du niveau de pouvoir le plus élevé dans votre entreprise (directeur, administrateur…) et à éviter tout conflit d'intérêt potentiel entre ses éventuelles autres missions et celles qu'il devra assumer en tant que DPO.

S'il s'agit d'un DPO externe, veillez à éviter les conflits d'intérêt éventuels et prenez en compte le risque qu'un externe puisse moins bien connaître votre entreprise et/ou puisse éprouver plus de difficultés à être en relation avec vos différents services.

Que le DPO soit interne ou externe, n'oubliez pas de rappeler dans son contrat que le DPO est tenu au secret professionnel et qu'il a une obligation de confidentialité en ce qui concerne l'exercice de ses missions[43].

Pensez également à communiquer les coordonnées du DPO à l'Autorité de protection des données et à les publier sur votre site web ainsi que dans vos documents officiels à destination de vos clients personnes physiques afin que les personnes concernées puissent le contacter[44].

Enfin, n'oubliez pas de former votre DPO (formation initiale et formation continue) !

Consultez régulièrement le site de l'Autorité de protection des données. Celle-ci publie de nombreux templates et guidelines destinés à vous aider.

41 Dans bien des cas, cette désignation est obligatoire : voir notamment art. 37 et suivants RGPD/GDPR. En admettant qu'une telle désignation ne soit pas obligatoire pour votre entreprise, elle est néanmoins fortement conseillée.

42 Voir notamment art. 39 RGPD/GDPR.

43 Art.38 RGPD.

44 Art. 37 RGPD.

Prévoyez une procédure de notification d'incident

a) Notification à l'Autorité de protection des données (art. 33 GDPR)

En principe, en cas de violation de données à caractère personnel, le responsable du traitement doit notifier la violation en question à l'Autorité de protection des données dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance. Lorsque la notification à l'Autorité de protection des données n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

Mieux vaut ne pas attendre et notifier la violation sans délai à l'Autorité de protection des données même si vous ne disposez pas de toutes les informations relatives à l'incident, quitte à fournir les détails au fur et à mesure que vous en disposerez.

Prévoyez dans vos contrats que le sous-traitant doit avertir le responsable du traitement dès qu'il a pris connaissance d'une violation de données à caractère personnel.

b) Notification aux personnes concernées (art. 34 GDPR)

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Cette notification aux personnes concernées n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :

- le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement[45];
- le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser ;
- la communication à chacune des personnes concernées exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace.

45 Voir Glossaire.

Si vous souhaitez diminuer fortement le risque, pensez aux mesures techniques telles que la cryptographie[46] : la notification aux personnes concernées ne doit se faire que lorsqu'il existe un risque élevé d'atteinte à leurs droits et libertés. Si vous avez eu recours à de bonnes clefs de cryptographie, ce risque élevé est fort peu probable.

Consultez régulièrement le site web de l'Autorité de protection des données.

Pensez également à consulter :

- ENISA : Guidelines for SMEs on the security of personal data processing (2017)
- Cybersecurity Coalition : GDPR Check up (2017)
- CNIL (France) : qui propose divers outils (registre, DPIA[47],...)
- BPI France et CNIL : Guide pratique de sensibilisation au règlement général de protection des données (2018)
- ICO (UK)

4.2.5. Principe 5. Organisez régulièrement des tests et des contrôles

Réalisez régulièrement un audit de vos mesures de sécurité. L'audit peut être interne ou externe. Evitez si possible les situations où votre référent numérique (conseiller en sécurité de l'information, Data Protection Officer, point de contact de votre personnel en cas d'incident IT) se contrôle lui-même. Mieux vaut disposer d'un peu plus de recul en faisant par exemple appel à un auditeur externe, au moins une fois par an, afin d'identifier si vos mesures de sécurité sont suffisantes et/ou si des points d'amélioration pourraient être apportés. Veillez toutefois à préciser dans le contrat qui vous unira à un auditeur externe non seulement le champ d'application exact des tests et contrôles mais également les règles en matière de sécurité et de confidentialité afin de protéger votre entreprise pendant le contrôle...et au-delà.

N'oubliez pas d'avertir votre équipe technique suffisamment à l'avance pour disposer d'un « point de recovery »[48] efficace en cas de souci.

Evitez de préférence de réaliser des tests sur des environnements de production.

Attention : des mesures particulières peuvent également s'appliquer si votre entreprise est désignée comme infrastructure critique ou opérateur de service essentiel.

46 Voir Glossaire.

47 Voir Glossaaire

48 Voir Glossaire.

N'hésitez pas à vous informer auprès de l'autorité nationale responsable pour votre secteur.

4.2.6. Principe 6. Mitigez vos risques et au besoin, assurez-vous !

En fonction des besoins de votre entreprise, mitigez c'est-à-dire limiter et/ou transférer une partie de vos risques : pensez notamment à évaluer si vous avez besoin de faire assurer votre entreprise contre les cyberrisques.

A l'heure actuelle, pour un prix relativement abordable, plusieurs assureurs proposent des produits adaptés. Le nom et le champ d'application des produits peuvent varier d'un assureur à l'autre : assurance contre les risques cybernétiques, cyberassurance...

Pensez à prendre connaissance de la couverture qui vous est proposée afin d'identifier celle qui correspond à vos besoins, vérifiez également si la responsabilité des administrateurs et dirigeants est couverte par ailleurs et si vous disposez d'une assurance vol et incendie couvrant vos outils (ordinateurs...).

Pour en savoir plus, consultez Cyber Insurance : Recent Advances, Good Practices and Challenges.

4.2.7. Principe 7. Concevez un « Incident Management Plan » réaliste

En matière de cyberincident, tout n'est qu'une question de temps : si vous n'avez pas encore été victime d'une cyberattaque, vous serez probablement le suivant. Autant se préparer dès maintenant en élaborant un « Incident Management Plan » !

Consultez l' Incident Management Guide de la Cyber Security Coalition.

4.2.8. Principe 8. Sécurisez les appareils mobiles

Pour vous aider, consultez le document Smartphone Secure Development Guidelines de l' European Network and Information Security Agency (ENISA, 2017).

4.2.9. Principe 9. Virtualisez en toute sécurité

Pour vous aider, consultez le document Security aspects of virtualization de l'ENISA (2017) et exploitez l'outil « Sécurité du Cloud » de l'ENISA .

Voir également « 4.2.10. Principe 10. Prévoir les relations avec les tiers ».

« Créer les conditions d'un fonctionnement compétitif, durable et équilibré du marché des biens et services en Belgique. »

4.2.10. Principe 10. Prévoyez les relations avec les tiers

N'oubliez pas de prévoir des niveaux similaires de sécurité tout au long de la chaîne de production. La sécurité de votre entreprise dépend aussi de la sécurité de vos fournisseurs.

Prévoyez des niveaux de service attendus avec vos fournisseurs de services (Service Level Agreement ou SLA) ainsi que les sanctions en cas de non-respect de ces niveaux de service.

Voici une liste non exhaustive de clauses que vous pourriez vouloir insérer dans vos contrats :

1. définir une phase test éventuelle : votre partenaire professionnel est-il fait pour vous ?
2. rappeler à votre sous-traitant qu'il est lui aussi tenu au respect du GDPR : votre sous-traitant a notamment l'obligation de vous aider à garantir le respect de vos obligations en matière de protection des données (vous avertir sans délai s'il constate une possible infraction, une éventuelle perte de données, contribuer à vous fournir l'information nécessaire pour votre analyse d'impact, veillez à respecter les règles de sécurité correspondant aux « règles de l'art »...)
3. identifier la localisation de serveurs (sont-ils situés en Europe ? Si les serveurs sont situés en dehors de l'Europe, n'oubliez pas toutes les précautions particulières à prendre si vous traitez des données à caractère personnel !) ;
4. la possibilité de consulter au moins une fois par an la liste des prix proposés par votre partenaire professionnel pour le même type de produits/services et pour un volume de biens/services suffisamment comparable au vôtre (meilleur prix);
5. définir des niveaux de services (SLA) : taux de disponibilité du système (en heures pour des jours ouvrables/non ouvrables) ; durée et occurrence maximale d'indisponibilité mensuelle, trimestrielle ou annuelle d'un composant ou du système ; temps de réponse moyen d'une application ou de certaines requêtes et durée maximale de certains traitements,... ;
6. exiger que, tout au long de la durée du contrat, le niveau de service le plus élevé offert à l'un des clients du fournisseur vous soit également proposé pour le même prix (upgrade).
7. disposer du calendrier des maintenances éventuelles (à temps pour que vos services puissent s'organiser) ;
8. organiser des audits de sécurité auprès du fournisseur (pensez à définir le périmètre, la périodicité, la prise en charge du coût, l'organisme auditeur indépendant et autorisé par les parties...) ;

9. garder un œil sur la sous-traitance de votre fournisseur :
    - soit interdire la sous-traitance de votre fournisseur sans accord préalable de votre entreprise quant à l'identité du sous-traitant envisagé et aux limites du contrat envisagé (si celui-ci est en lien avec l'exécution de votre contrat) ;
    - soit demander à être tenu au courant de toute sous-traitance pouvant impacter les services qui vous sont offerts et exiger que les obligations et précautions précisées dans le contrat avec votre fournisseur soient également prévues dans les contrats de sous-traitance pouvant en découler (les mêmes règles doivent s'appliquer aux sous-traitants de votre fournisseur);
10. se préparer à un incident :
    - demander les journaux d'incidents et l'accès à la conservations des traces (logs)
    - disposer des indicateurs sur l'historique du service hébergé comme la fréquence et le suivi des mises à jour effectuées (indispensable), la durée d'indisponibilité maximum et le suivi de ces indisponibilités...
    - assurer le suivi en cas d'incident : identité de la personne de contact et des moyens de la contacter (7j/7, 24h/24) aussi bien chez vous qu'auprès de votre fournisseur ; avertissement sans délai en cas d'attaques ; définition des matrices d'escalade[49], définition de ce que l'on entend par « incident » ;
    - interdire ou non certaines actions postérieures à un incident sans accord préalable de votre part (arrêt, démarrage, rétablissement d'une sauvegarde, isolement physique du reste du réseau, effacement des journaux d'incidents...)
11. prévoir la fin de vos relations (clause de réversibilité) :
    - cette clause doit vous permettre de reprendre la gestion de la fonction externalisée, soit pour l'exploiter directement, soit pour en confier l'exploitation à un (nouveau) tiers de votre choix.
    - le prestataire devrait s'engager à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par votre entreprise ou par un autre prestataire de service désigné par votre entreprise.
    - à la fin de l'exécution du présent contrat, le titulaire pourrait par exemple être tenu :
        - » de vous transférer les informations sur le contexte fonctionnel et technique de l'ensemble applicatif ainsi que sur les aspects de suivi du projet ;
        - » de préparer un support informatique défini en collaboration avec vos services et contenant tous les éléments (documentation, programmes, chaînes

49 Voir Glossaire

de compilation...) gérés par le fournisseur actuel et qui seront, à l'issue de cette prestation, placés sous votre responsabilité ou celle de votre futur fournisseur ;

» de garantir, lors du transfert, la sécurité des données et des applications qui lui ont été confiées, conformément à ses obligations ;

» de ne pas modifier la qualité, les termes et les conditions des services jusqu'à lors fournis à votre entreprise sans un accord exprès de votre part une fois la phase de réversibilité entamée ;

» en cas d'arrêt des prestations confiées par votre entreprise, de détruire ou restituer l'ensemble des matériels, logiciels et documentation qui lui ont été confiés (pensez à prévoir un dernier audit pour vérifier que votre ancien fournisseur s'est bien exécuté) ;

» d'assurer une formation fonctionnelle approfondie (identifier le nombre d'heures minimum/maximum) soit à votre personnel soit à celui du futur fournisseur, avec travaux pratiques sur poste de travail, en présence de représentants de votre entreprise. Cette formation devra s'appuyer sur la documentation « utilisateurs » et la documentation technique rédigées par votre fournisseur.

Si vous traitez des données à caractère personnel, voyez également le point « 4.2.4 Principe 4. Prévoyez les dispositions en matière de protection de la vie privée ».

Vous ne comprenez pas certains termes employés ? Consultez notre glossaire.

4.3. Etape 3. 12 actions

N'hésitez pas à consulter le Guide pour les PME réalisé par la Cyber Security Coalition en collaboration avec le Centre pour la Cybersécurité Belgique (CCB). Il présente des informations utiles concernant les 12 points d'action suivants.

4.3.1. Action 1. Top management impliqué

Donnez l'exemple à vos employés ! Montrez que vous comprenez les risques et que vous envisagez votre stratégie de sécurité de l'information en même temps que votre stratégie organisationnelle.

Pour être cohérent, n'oubliez pas :

- d'identifier vos actifs ;
- de définir vos priorités (objectifs) ;

- d'indiquer des mesures de performance des actions que vous avez soutenues au sein de votre entreprise (KPI) ;
- de désigner une ou plusieurs personnes afin de remplir les fonctions pertinentes pour votre entreprise et liées à la sécurité de l'information.

4.3.2. Action 2. Elaborez une politique de sécurité et un code de conduite

a) Politique de sécurité

Pour dresser votre politique de sécurité, l'idéal est de faire appel à des méthodologies éprouvées. Pour en savoir plus, voir le « point 8. Principaux standards, Sécurité de l'information» et le point « 4.2.2. Principe 2. Sensibilisez votre personnel à la sécurité de l'information. Une fois votre politique de sécurité dressée, n'oubliez pas de rallier vos utilisateurs à votre politique !

b) Code de conduite

Si vous souhaitez dresser un code de conduite qui respecte votre politique de sécurité, voici quelques éléments à prévoir :

Les accès à vos ressources :

- Qui peut accéder à votre réseau internet ? A votre réseau intranet ? A vos espaces de stockage ?
- Qui peut accéder à/partager vos documents/données ?

Les utilisations non désirées de votre réseau ou de votre espace de stockage :

- consultation de sites pornographiques, de sites pédophiles ou de sites dont le contenu est susceptible de porter atteinte à la dignité d'autrui ;
- envoi d'e-mails à des fins lucratives/commerciales sans rapport avec votre entreprise ;
- envoi d'e-mails avec l'intention de nuire à leur expéditeur ou à l'auteur du courrier électronique initial ;
- envoi d'e-mails de nature à nuire aux intérêts de votre entreprise ;
- conservation de fichiers personnels sur le matériel mis à la disposition des utilisateurs et notamment utilisation de l'espace de stockage professionnel à des fins personnelles ;
- envoi de fichiers avec des pièces jointes volumineuses (préciser la taille maximale autorisée des fichiers).

Les « règles de base » en matière de déontologie. Par exemple :

- se conformer aux directives données par l'employeur ainsi qu'à la politique sur la sécurité de l'information ;
- utiliser, dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels (par exemple, les données) mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés ;
- respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ou les désactiver ;
- se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ce qui implique, notamment, de respecter les conditions d'utilisation des licences et de ne pas installer de logiciel (software) sur le matériel fourni par l'employeur sans accord préalable de ce dernier ;
- signaler immédiatement à leur supérieur ou au point de contact désigné tout acte dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de l'entreprise ;
- au moment de leur départ de l'entreprise, remettre les différentes cartes d'accès (badges…), les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions ;
- le membre du personnel doit utiliser ses moyens d'authentification personnels. Ceux-ci ne peuvent pas être communiqués ou confiés à une tierce personne sauf procédure particulière afin d'assurer la continuité du service (départ subit, maladie prolongée…) ;
- le membre du personnel ne peut pas bloquer/retarder la mise à jour automatique des programmes antivirus et des logiciels informatiques métier mis à sa disposition ;
- le membre du personnel remplit ses fonctions avec loyauté, conscience et intégrité sous l'autorité de ses supérieurs hiérarchiques et fonctionnels. A cet effet, il est tenu de respecter les lois et règlements en vigueur ainsi que les directives de l'autorité dont il relève. Le membre du personnel est en outre également tenu à un devoir général de loyauté vis-à-vis de son employeur ;
- le membre du personnel évite tout comportement ou tout acte qui pourrait nuire à l'efficacité de son travail ;

- le membre du personnel évite, en dehors de ses fonctions, tout comportement ou propos qui pourrait ébranler la confiance du public dans l'entreprise. Il s'agit notamment des comportements et propos qui ne seraient pas respectueux des principes démocratiques, énoncés notamment par la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, la loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme et la xénophobie et la loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste allemand pendant la seconde guerre mondiale et la Convention relative aux droits de l'enfant adoptée à New York le 20 novembre 1989 ;
- le membre du personnel ne peut, en aucune façon, tirer profit de sa fonction pour solliciter, exiger ou recevoir, directement ou par personne interposée, même en dehors de ses fonctions mais en raison de celles-ci, des dons, des gratifications ou des avantages quelconques ;
- le membre du personnel ne peut traiter un dossier dans lequel il a, directement ou indirectement, un intérêt fonctionnel ou personnel ;

- le membre du personnel veille à établir, dans la mesure du possible, une relation de confiance avec le client. Il fait preuve, dans l'exercice de ses fonctions, de disponibilité et de diligence. Le membre du personnel doit utiliser, dans ses rapports avec le client, quelle qu'en soit la forme, un langage compréhensible pour le public. Le membre du personnel traite le client avec courtoisie, respect, compréhension et sans aucune discrimination, en respectant les principes démocratiques énoncés notamment par la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales.

Le traitement de données à caractère personnel (voir également le point « 4.2.4 Principe 4. Prévoyez les dispositions en matière de protection de la vie privée»). Par exemple :

- le membre du personnel traite les données à caractère personnel dans le respect des dispositions des règles relatives à la protection de la vie privée à l'égard des traitements de données à caractère personnel et notamment, dans le respect du règlement général sur la protection des données (règlement 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE).
- le membre du personnel ne peut faire usage des données à caractère personnel auxquelles il a accès aux fins d'obtenir directement ou indirectement un avantage pour lui-même ou pour autrui.
- sauf exception prévue par le règlement général sur la protection des données, le membre du personnel ne peut s'opposer à la demande d'un client (personne physique) de consulter les données à caractère personnel qui le concerne. Le membre du personnel est invité à suivre la procédure prévue à cet effet.

4.3.3. Action 3. Sensibilisez vos travailleurs aux risques cyber

- Rappelez régulièrement aux utilisateurs l'importance d'un comportement sain et sûr en matière de sécurité de l'information.
- Rappelez régulièrement aux utilisateurs que les informations doivent être considérées comme sensibles et traitées dans le respect des règles de protection de la vie privée.
- Informez les collaborateurs du service comptabilité au sujet du phénomène de « fraude au CEO » et prévoyez des procédures de contrôle dans le cadre de l'exécution des paiements.
- Informez les utilisateurs sur la façon de reconnaître le phishing (fraude par e-mail) et la réaction à adopter.

- Evaluez périodiquement la sensibilisation et la réactivité des utilisateurs voire intégrez les notions de connaissance et de respect de votre politique de sécurité de l'information dans l'évaluation du personnel.

Pour en savoir plus, consultez le point « 8.2 Gestion des risques » et plus particulièrement la norme ISO/IEC 27005:2011 Information security risk management.

Vous pouvez également consulter le site web de Febelfin concernant les risques bancaires.

4.3.4. Action 4. Gérez vos ressources informatiques importantes

- Maintenez une carte détaillée et actualisée de tous vos réseaux et interconnexions.
- Tenez un inventaire de l'ensemble des équipements ICT et des licences de logiciels.
- Assurez-vous de définir correctement les niveaux de service que vous attendez et de mettre en place des sanctions efficaces en cas de dégradation/rupture de services (SLA Service Level Agreement). Le cas échéant, désignez un Service Level Manager.
- Auditez régulièrement toutes les configurations (y compris les serveurs, les pare-feu et les composants de réseau).
- Identifiez les compétences clefs et les personnes qui en disposent au sein de votre entreprise.
- Implémentez un processus de contrôle du changement (Change/Release Manager).

4.3.5. Action 5. Mettez à jour tous les programmes

- Procédez aux mises à jour automatiques de sécurité de tous les logiciels et introduisez une culture interne du patch[50] (postes de travail, appareils mobiles, serveurs, composants réseau...).
- Effectuez un back-up complet des serveurs avant la mise à jour et créez des disques de réparation d'urgence après la mise à jour.

4.3.6. Action 6. Installez une protection antivirus

- Installez un logiciel antivirus sur tous les serveurs, postes de travail et appareils mobiles.
- Mettez automatiquement à jour vos antivirus.

50 Voir Glossaire.

- Disposez d'une personne experte (interne et/ou externe) qui puisse analyser les incidents et alertes.
- Vérifiez l'efficacité de votre antivirus via : http://www.eicar.org

4.3.7. Action 7. Sauvegardez toutes les informations

- Sauvegardez vos données importantes quotidiennement.
- Stockez vos sauvegardes hors ligne et à un endroit séparé (si possible, éloignées de leur source).
- Hébergez vos solutions de sauvegarde sur vos propres serveurs ou dans le cloud mais pensez à les sécuriser de manière adéquate et si possible à crypter vos données.
- Effectuez régulièrement des tests de restauration pour évaluer la qualité de vos sauvegardes et de vos processus.

4.3.8. Action 8. Gérez les accès à vos ordinateurs et réseaux

- Maintenez une liste limitée et actualisée des comptes d'administrateur du système et exercez une surveillance accrue des activités sur ces comptes (cibles privilégiées).
- Assurez-vous que les utilisateurs ne sont autorisés à accéder qu'aux informations dont ils ont besoin pour effectuer leurs missions (mettez en place un IAM[51]).
- Réalisez régulièrement un audit sur le répertoire central (Active Directory ou LDAP [52] directory).
- Empêchez tout direct accès à internet. Forcez le passage par un proxy[53] et IDS[54].
- Détectez les accès irréguliers aux informations et aux systèmes (délais, applications, données...).
- Privilégiez l'authentification multifactorielle (par exemple avec plusieurs facteurs comme mots de passe et code transféré via SMS...)
- Adoptez une politique de mots de passe efficace pour les utilisateurs.
- Pensez à modifier tous les mots de passe originaux sur les hardware et software qui vous sont fournis (routers, firewall...).

51 Voir Glossaire

52 Voir Glossaire

53 Voir Glossaire

54 Voir Glossaire

- Modifiez les paramètres de votre firewall (pare-feu) en fonction des besoins de votre entreprise.
- Limitez le nombre de tentatives autorisées pour vous connecter à votre réseau d'information (par exemple 3 tentatives).
- Désactivez immédiatement les comptes non utilisés.
- Organisez le nettoyage de bureaux pendant les heures de travail ou sous surveillance permanente.

4.3.9. Action 9. Sécurisez les postes de travail et les appareils mobiles

- Désactivez la fonction « Autorun » de médias externes.
- Interdisez la connexion des appareils personnels (BYOD[55]) au système d'information de l'organisation.
- Empêchez techniquement la connexion des supports portables non enregistrés OU installez un programme antivirus automatique pour tous les lecteurs de media externes (USB...).
- Maintenez une « liste blanche » des programmes permis ainsi qu'une « liste noire » des programmes interdits.
- Rappelez régulièrement au personnel toute l'importance de ne jamais laisser sans surveillance le matériel mis à leur disposition (GSM, PC, tablette...).
- Installez un verrouillage automatique après quelques minutes sans utilisation des postes de travail et des appareils mobiles.
- Cryptez les informations se trouvant sur vos serveurs, sur vos clouds ainsi que les disques durs des ordinateurs portables.
- Les données sensibles ou confidentielles ainsi que les données à caractère personnel devraient idéalement être transmises sous forme cryptée.
- Stockez et assurez-vous de disposer d'une copie de toutes les données professionnelles dont vous pourriez avoir besoin.
- Si vous avez recours à un fournisseur de cloud, assurez-vous que les garanties offertes par votre fournisseur correspondent au niveau de criticité des informations stockées.
- Détruisez les disques durs, les médias et les imprimantes déclassés contenant des données OU assurez-vous de les avoir nettoyés correctement, entièrement et plusieurs fois avant d'en faire don à une association caritative.

55 Voir Glossaire.

- Evitez de préférence d'autoriser que des programmes « .exe » puissent s'exécuter sans votre accord préalable.

4.3.10. Action 10. Sécurisez les serveurs et les composants de réseau

- Utilisez des applications et des protocoles sécurisés.
- Imposez le VPN[56] pour les connexions à distance.
- Changez tous les mots de passe par défaut et désactivez les comptes non utilisés.
- Fermez les ports et services non utilisés.
- Restreignez l'accès physique aux serveurs et aux composants de réseau à un nombre minimum de personnes.
- Enregistrez tout accès physique aux serveurs et aux composants de réseau.
- Utilisez un réseau (logiquement) distinct du réseau de l'utilisateur pour l'administration des serveurs.
- Assurez-vous de disposer d'un système IDS/IPS[57] (Intrusion Detection/Prevention System).
- Conservez les journaux de sécurité sur les serveurs et les pare-feu de préférence 6 mois.
- Assurez-vous de disposer d'un SIEM[58] afin de détecter tout comportement malveillant.
- Evaluez tous les évènements et alertes des serveurs, pare-feu et composants de réseau.
- Exécutez des tests d'intrusion et des scans de vulnérabilité.
- Renforcez tous les systèmes conformément aux recommandations du fournisseur.
- Protégez le wi-fi de votre entreprise par des technologies récentes et régulièrement mises à jour (WPA2 Enterprise) et enregistrez vos appareils.
- Séparez l'éventuel réseau wi-fi public du réseau de votre entreprise.
- Protégez votre nom de domaine contre le « spoofing ».

56 Voir Glossaire.

57 Voir Glossaire.

58 Voir Glossaire.

4.3.11. Action 11. Sécurisez les accès à distance.

- Limitez l'accès à distance au strict nécessaire.
- L'accès à distance doit être fermé automatiquement en cas d'inactivité pendant un certain temps.
- Imposez une authentification forte lors d'une connexion à partir de réseaux publics extérieurs.
- N'autorisez que des connexions de Virtual Private Network (VPN[59]) à partir de points finaux.
- Sécurisez et cryptez toutes les connexions au réseau d'entreprise.

4.3.12. Action 12. Disposez d'un plan de continuité des activités (BCP) et d'un plan de gestion des incidents

- Disposez d'un plan de gestion des incidents afin de répondre à un incident et faites des exercices réguliers pour en tester l'efficacité (minimum une fois par an).
- Disposez d'un plan de continuité des activités afin de préserver l'entreprise.
- Evaluez et testez ces plans annuellement.
- Installez des dispositifs d'urgence pour les services d'utilité (électricité, téléphone, Internet...).
- Evaluez l'opportunité d'une assurance contre les incidents de cyber sécurité.
- Pour en savoir plus sur ces actions, vous pouvez consulter le site web du Centre pour la Cybersécurité Belgique (CCB), les publications en matière d'incident management sur le site de l'ENISA, ainsi que l'Incident Management Guide publié par la CyberSecurity Coalition.

59 Voir Glossaire

5. Top 10 des incidents

Chaque année, les différents Computer Emergency Response Team (CERT[60]) des Etats membres publient les statistiques relatives aux incidents constatés sur leur territoire.

L'ENISA (European Network and Information Security Agency) compile ensuite les informations et publie un rapport annuel présentant les menaces constatées en Europe. Certaines grandes catégories (malwares) peuvent recouvrir d'autres types d'incidents (ransomwares, phishing...).

Voici le top 10 des incidents les plus constatés en Europe en 2017 ainsi que quelques bons réflexes à acquérir en fonction du type d'incident.

5.1. Malware

Les malwares[61] les plus fréquents en 2017 ont été les ransomwares [62]et les vols d'informations mais il en existe bien d'autres : chevaux de Troie[63] (Trojans), PUPs[64]

60 ou Computer Security Incident Response Team (« CSIRT »)

61 Voir Glossaire

62 Voir Glossaire

63 Voir Glossaire.

64 Voir Glossaire.

© momius - Fotolia.com

(Potentially Unwanted Programs), droppers[65], Command & Control[66] (C&C), key loggers[67], backdoors....

Les bons réflexes sont notamment :

- ne pas se reposer sur un anti-malware unique (privilégier multi-scanner/multi-canaux) ;
- prévoir une détection sur les différents canaux utilisés (intranet, internet, plateformes, PC, GSM...) ;
- prévoir une politique de sécurité et un incident management plan avec un point concernant les malwares ;
- prévoir des outils d'analyse sur les malwares et se tenir informés des dernières tendances ;
- réaliser des tests réguliers et mettre en place un monitoring.

65 Voir Glossaire.

66 Voir Glossaire.

67 Voir Glossaire.

5.2. Web-based attacks

Les attaques « Web based attacks » portent en général sur les browsers[68] (Google, Mozilla, Safari…) et sur leurs extensions ainsi que sur les systèmes de gestion des contenus (Content management Systems ou CMS comme WordPress, Drupal, Joomla…).

Les bons réflexes consistent notamment :

- à mettre à jour (patcher) régulièrement afin d'appliquer les correctifs de sécurité ;
- à prévoir une protection contre les softwares connus pour être vulnérables et non patchés ;
- à préférer une identification à plusieurs facteurs (politique des mots de passe…) ;
- à modifier le préfixe par défaut de la base de données (par exemple wp_ pour WordPress) ;
- à prévoir un point de restauration régulier ;
- à détecter et filtrer les browsers[69] plug-ins (ne provenant pas de sites officiels).

5.3. Web application attacks

Les attaques « Web application » sont des attaques portant sur les applications web et les services web. Elles exploitent le plus souvent de mauvaises configurations ou des vulnérabilités dans les composants ou dans l'infrastructure.

Les attaques les plus fréquentes sont des injections de code SQL, des injections PHP, des Local File Inclusion (FLI), des cross site scripting (XSS)…

Les bons réflexes sont notamment :

- d'établir une politique de sécurité concernant le développement et la mise en production des applications ;
- de recourir à des mécanismes d'authentification et d'autorisation répondant aux règles de l'art ;
- d'installer un web application firewalling (WAF)[70] permettant de vérifier les données HTML, HTTPS, SOAP, XML-RPC ;

68 Voir Glossaire.

69 Voir Glossaire.

70 Voir Glossaire.

- de filtrer le trafic en vérifiant les performances sur les différents canaux (intranet, internet, mails…) ;
- de scanner régulièrement et faire des tests de détection d'intrusion.

Pour en savoir plus, vous pouvez notamment consulter :

- le site securitymadein.lu
- le livre blanc du CERT.eu

5.4. Phishing

Le Phishing[71] (ou tentative d'hameçonnage) est un type d'attaque qui prend la forme d'un mail alarmant (suppression de votre compte, facture à payer avant saisie…) semblant provenir d'une entreprise connue et de confiance (banques, pouvoirs publics, fournisseurs de services…).

L'objectif est de soutirer des informations personnelles à l'utilisateur (données bancaires, nom des comptables de l'entreprise…).

71 Voir Glossaire.

Parfois, le courrier électronique contenant une reproduction du logo de l'entreprise usurpée envoie la victime sur un site web qui a également été usurpé ou invite la victime à ouvrir une pièce attachée infectée. L'e-mail et le site semblent authentiques et dans certains cas l'adresse URL est masquée de telle sorte qu'elle semble correcte.

Parmi les bons réflexes, citons notamment :

- organisation d'une campagne de sensibilisation des employés concernant le phishing (voir kit de sensibilisation à destination des PME) ;
- filtrage des e-mails ;
- vérification DNS ;
- détection et suppression des pièces attachées infectées ;
- détection des caractéristiques des liens URL malicieux ;
- détection des fraudes et anomalies sur le réseau ;
- authentification multifactorielle obligatoire pour tous les éléments critiques (gestion des comptes bancaires...).

Vous pouvez également dénoncer la tentative de phishing via le lien suivant : suspect@safeonweb.be.

En dénonçant l'adresse d'un site de phishing, chaque site fera l'objet d'une validation et s'il s'agit bien d'une tentative de phishing, les browsers seront tenus au courant et bloqueront les adresses problématiques dans les navigateurs. Vous contribuerez ainsi à diminuer l'impact de ce type de tentative en empêchant que d'autres internautes soient à leur tour victimes de la fraude.

Vous pouvez également vérifier une adresse URL via cet outil

5.5. SPAM

Il s'agit d'un type d'attaque ayant le plus souvent recours à un botnet[72] pour lancer massivement des e-mails malicieux transportant des malwares (fichiers exécutables...).

Les spams ont gagné en qualité en 2017, par exemple en combinant des informations pour mieux piéger leurs victimes tout en ayant recours à certaines techniques afin d'éviter les filtres anti-spams.

72 Voir Glossaire.

La majorité des spams proposent un contenu relevant de l'une des catégories suivantes :

- contenu adulte (à caractère sexuel) ;
- lettres en chaine ;
- santé et pseudo – produits pharmaceutiques ;
- IT et pseudo virus ayant infecté votre système ;
- bancaires (demandes « urgentes » impliquant le transfert de données bancaires) ;
- fausses victoires de loterie ;
- lettres nigérianes (demande d'assistance dans le mouvement/transfert de fonds monétaires étrangers) ;
- éducation (promesses de bourses dans de grandes universités...).

Parmi les bons réflexes, citons notamment :

- dresser la liste des spammers connus[73] et bloquer tout mail provenant de leur botnet ;
- utiliser des filtres adaptés (filtre de réputation, de contenu, RBL, anti-spam, anti-malware...) ;
- bloquer les fichiers exécutables (.exe) attachés dans les e-mails ;
- empêcher l'exécution automatique de codes, macros, graphiques, etc. ;
- sensibiliser les employés (ne pas ouvrir les pièces attachées de mails suspects...) ;
- scanner et filtrer les mails avec pièces attachées.

5.6. DDoS

Les attaques par déni de service (Distributed Denial of Service) sont menées contre un site web ou un serveur et ont pour objectif de l'empêcher de continuer à fonctionner correctement et d'empêcher les utilisateurs légitimes d'un service de l'utiliser de manière normale. Pour être efficace, ce type d'attaque repose le plus souvent sur un grand nombre d'objets connectés infectés (botnet[74]). En raison du nombre gigan-

73 Une liste des 10 spammers mondiaux les plus connus est régulièrement mise à jour et gratuitement disponible sur le site de SPAMHAUS : https://www.spamhaus.org/statistics/spammers/

74 Voir Glossaire.

tesque d'informations, le site web ou le serveur attaqué ne peut plus traiter les innombrables requêtes et n'est dès lors plus accessible.

Le nombre grandissant d'objets connectés (IoT)[75] qui peuvent être autant de points de vulnérabilité permettant d'être contrôlés par des cyberattaquants laisse malheureusement présager que ce type d'attaques pourrait devenir de plus en plus fréquent.

Parmi les bons réflexes, citons notamment :

- prévoir une politique de sécurité et un Incident Management Plan avec un point concernant les attaques DDoS ;
- avoir de préférence recours à un fournisseur d'accès à internet (FAI ou ISP) qui implémente des mesures de protection contre les attaques DDoS ;
- avoir recours à des outils spécifiques : Firewall based, Access Control Lists (ACLs), Load-balancer, IPS/WAF, Intelligent DDoS mitigation systems (IDMS), Cloud-based DDoS mitigation service…
- contrôles et tests sur les mesures prises par l'entreprise et sur ses capacités de réaction ;
- prévoir un Intrusion Prevention System (IPS) car certaines attaques DDoS peuvent masquer une tentative d'intrusion.

Pour en savoir plus, consultez :

- le livre blanc du Cert.be DDoSProactive and Reactive measures
- la page Attaques DDos : comment se protéger
- le livre blanc du Cert.eu : DDoS : Overview and Response Guide (2017)

5.7. Ransomware

Un ransomware est un programme malveillant qui encrypte les données figurant sur l'appareil infecté tout en promettant de restituer les données moyennant paiement d'une rançon (en bitcoins).

Pour plus d'infos, consultez :

- le site No more ransom !
- le site Ransomfree.cybereason

75 Voir Glossaire.

© zephy_P - Fotolia.com

Parmi les bons réflexes, citons notamment :

- disposer d'une bonne gestion des back-up (copies de sauvegarde, de préférence stockée ailleurs) ;
- disposer d'un antivirus efficace ;
- mettre à jour son système d'exploitation (OS) et ses applications ;
- activer la fonction « Afficher l'extension des noms de fichiers » dans la configuration du système d'exploitation (OS)[76] de vos ordinateurs. Cela vous aidera à repérer plus facilement les fichiers potentiellement malveillants. Méfiez-vous des extensions telles que « .exe », « .vbs » et « .scr ». Les escrocs peuvent utiliser différentes extensions pour camoufler un fichier malveillant en vidéo, photo ou document (comme hot-chics.avi.exe ou doc.scr) ;
- si vous découvrez un processus scélérat ou inconnu sur votre machine, déconnectez-la immédiatement de l'internet ou de tout autre connexion réseau (comme le wi-fi de votre entreprise), cela empêchera l'infection de se propager en attendant l'intervention d'une équipe technique.

76 Voir Glossaire.

- penser à consulter les sites spécialisés qui peuvent vous proposer de bons conseils et outils en matière de prévention ainsi qu'en matière de nettoyage des appareils infectés
  - » https://www.nomoreransom.org/
  - » https://ransomfree.cybereason.com/

Pour en savoir plus, consultez également le guide Ransomware. How to protect and respond du CERT.

5.8. Botnets

Un botnet est un réseau d'objets connectés (« armée d'appareils zombies ») qui sont utilisés – souvent à l'insu de leurs propriétaires – pour attaquer des sites web ou des serveurs d'entreprises et d'organisations en bombardant les victimes de requêtes ou de malwares (voir DDoS, e-mails avec pièces attachées malicieuses…).

N'importe quel objet connecté à internet peut faire partie d'un botnet. Le processus est le suivant : un programme malveillant contamine un objet connecté à internet mais reste invisible sur celui-ci. Il attend un ordre des cybercriminels. A partir du moment où les cybercriminels ont contaminé suffisamment d'objets connectés, ils donnent l'ordre aux objets infectés de bombarder un site web ou un serveur déterminé. Des botnets peuvent aussi être loués à d'autres cybercriminels en passant sur le Dark web.

Parmi les bons réflexes, citons notamment :

- installation et configuration du réseau et firewall ;
- analyse des performances du trafic sur l'ensemble des canaux utilisés (intranet, internet, e-mails…) ;
- installation de black-list des adresses IP infectées détectées[77] ;
- installation d'un Botnet Sinkholing (la détection d'une attaque via botnet permet de rediriger les attaques vers un serveur martyr qui servira à collecter des données sur l'attaque lancée).

77 Une liste des principaux botnets mondiaux est régulièrement mise à jour et gratuitement disponible sur le site de SPAMHAUS.

5.9. Insider Threat

L'insider threat[78] ou « menace de l'intérieur » relève le plus souvent de la négligence ou d'une simple maladresse mais il peut également s'agir d'un acte malveillant de la part de l'un de vos (ex)employés.

Parmi les bons réflexes, citons notamment :

- comptes administrateurs limités et implémentation d'un Privileged Identity Management (PIM)[79] ;
- mise en place d'un Identity and Access Management (IAM)[80] (définition des rôles) ;
- sensibilisation de vos employés au sujet de ce qu'ils peuvent/ne peuvent pas faire avec les outils de travail qui leur sont confiés ;
- politique de sécurité prévoyant un point particulier en cas de licenciement de l'un/de plusieurs de vos employés ;
- mise en place d'une gouvernance des risques sur la base des différentes fonctions ;
- outils d'analyse des données ;
- monitoring des usagers (abus des droits fixés) et audit régulier.

5.10. Dommage physique, perte ou vol

Bien qu'il ne s'agisse pas à proprement parler d'un risque cyber, les dommages physiques représentent une menace importante.

Il peut s'agit de la perte/du vol de clefs USB sur lesquelles d'importantes informations non cryptées ont été stockées, de vols de serveurs (salle non protégée), de vols de GSM sur lesquels figurent des dossiers ou des e-mails contenant des informations importantes, de non- renouvellement des contrats de maintenance avec pour conséquence des serveurs en panne, des batteries de secours qui ne prennent pas le relais en cas de rupture de courant...

78 Voir Glossaire.

79 Voir Glossaire.

80 Voir Glossaire.

Parmi les bons réflexes, citons notamment :

- crypter toutes les informations devant se trouver sur des supports mobiles (GSM, clefs USB...) ainsi que sur votre réseau ;
- tenir un tableau des contrats de maintenance avec retroplanning afin de les renouveler endéans les temps ;
- tenir un inventaire des supports autorisés (et interdire les autres supports) ;
- établir des procédures pour les employés afin qu'ils sachent comment réagir en cas de vol de matériel (PC, GSM, USB...) et sensibiliser votre personnel ;
- si besoin, se faire couvrir par une assurance adaptée pour le vol et les risques cyber.

Pour en savoir plus, vous pouvez notamment consulter CIRCLean - USB key sanitizer.

Pensez à consulter les sites plus spécialisés dans les alertes techniques afin d'être tenu au courant des dernières tendances en ce qui concerne les vulnérabilités et les menaces :

ENISA

CERT.be

US-CERT

CASES

6. En cas d'incident, que faire ?

Si vous possédez un plan adapté (Incident Management Plan, Disaster Recovery Plan…), appliquez les règles prévues en fonction du type d'incident (voir également le point 8. Principaux standards).

N'hésitez pas à prendre contact avec le CERT.be[81] .

QUI CONTACTER ?

Police

N'hésitez pas à déposer une plainte auprès de la Police locale, celle-ci pourra ensuite transférer l'information auprès des autorités de police compétentes à savoir la Federal Computer Crime Unit (FCCU) ou la Regional Computer Crime Unit (RCCU) dont vous dépendez.

Vous pouvez vous rendre auprès de votre commissariat de quartier ou contacter la Police via les numéros suivants : 112 ou 101.

81 Voir rubrique « Qui contacter ? ».

Computer Emergency Response Team (CERT)

Que vous décidiez de déposer une plainte auprès de la Police ou non, contactez la Computer Emergency Response Team qui vous donnera les premiers conseils en cas d'incident.

Site officiel : https://www.cert.be/fr/welcome.html

E-mail : cert@cert.be.

Téléphone : +32 2 501 05 60 (jours ouvrables de 9h à 17h).

Autorité de protection des données (APD)

L'Autorité de protection des données est l'autorité nationale compétente pour toutes les atteintes relatives aux traitements de données à caractère personnel.

Les mesures de protection techniques et organisationnelles appropriées permettent de détecter rapidement si une violation des données à caractère personnel s'est produite et, si tel est le cas, permettent à l'entreprise responsable du traitement des données de réagir rapidement et d'informer sans délai l'Autorité de protection des données et, le cas échéant, les personnes concernées.

Si vous êtes sous-traitant au sens des dispositions relatives à la protection de la vie privée, n'oubliez pas d'avertir sans délai le responsable du traitement !

L'Autorité de protection des données doit être avertie des violations de données sans délai et au plus tard dans les 72 heures après la découverte de l'incident concernant des données à caractère personnel.

Site officiel : https://www.autoriteprotectiondonnees.be/

Adresse :

Autorité de protection des données
Rue de la Presse 35
1000 Bruxelles

Tél : +32 2 274 48 00 ou +32 2 274 48 79
E-mail : contact@apd-gba.be

Les bureaux de l'Autorité sont accessibles tous les jours ouvrables, sur rendez-vous.

L'Autorité de protection des données vous propose également un formulaire en ligne sur leur site web.

Autorité nationale responsable pour votre secteur

En fonction du secteur dont vous dépendez, voyez si vous devez avertir l'autorité nationale responsable pour votre secteur (IBPT, BNB...).

7. En savoir plus ? Acteurs et liens utiles

Vous voulez en savoir plus en matière de cybersécurité ?

Acteurs

En Belgique

Autorité de protection des données

CERT.be

Police, FCCU/RCCU : contactez la police de votre quartier.

En Europe et pays alliés

CERT.eu : Computer Emergency Response Team européenne, le CERT.eu produit des lignes directrices (guidelines) et des livres blancs (white papers) en matière de cybersécurité. Il identifie également les principales cybermenaces au niveau européen.

ECSO : association sans but lucratif (ASBL) créée à l'initiative de la Commission européenne et permettant au secteur privé et au secteur public de faire valoir leurs points de vue en matière de cybersécurité.

ENISA : (European Union Agency for Network and Information Security), l'ENISA publie de nombreux documents en matière de cyber sécurité à l'attention des entreprises et notamment des guidelines en matière de traitement de données à caractère personnel (GDPR/RGPD) ou de gestion des clouds. Voir également le glossaire, le quizz concernant la cybersécurité et la protection de la privée ainsi que les exercices d'entrainement à destination des cyberexperts de votre entreprise.

Liens utiles

ANSSI : site officiel français en matière de cybersécurité. L'ANSSI offre gratuitement une formation en ligne en matière de cybersécurité et dresse la liste des produits cyber qui ont passé leurs tests avec succès.

Cases (LU) : site officiel luxembourgeois en matière de cybersécurité. Voir notamment l'outil d'auto-évaluation, le système START/FIT/TOP et l'analyse de risques MONARC.

Centre pour la Cybersécurité Belgique (CCB)

CNIL (FR) : site officiel français offrant des conseils, documents et outils pour implémenter correctement le règlement général sur la protection des données (RGPD/

GDPR). La CNIL a également publié un guide RGPD à l'attention des PME/TPE ainsi que des documents concernant l'analyse d'impact relative à la protection des données (DPIA) et la liste des outils de sécurité ayant passé avec succès leurs tests.

CyberSecurity Coalition : la coalition propose notamment un cyberguide, un kit de sensibilisation à la cybersécurité, un premier questionnaire de maturité vis-à-vis du GDPR.

FEB : propose un guide de cybersécurité, une publication sur le GDPR et organise de nombreux events liés à la cybersécurité.

IASME : site anglais (UK) proposant d'autres questionnaires d'auto-évaluation.

IBPT : fournit des informations publiques sur les télécommunications (couverture des différents réseaux...).

ICC : La Chambre internationale de commerce a publié un Guide ICC de la cybersécurité à l'intention des entreprises sur lequel s'appuie le présent manuel pour la section Entreprise 1.0

INFOSEC : est un groupe d'experts qui propose des events ciblés sur différentes problématiques en matière de cybersécurité (cryptographie, 5G, IoT...).

NCSC (NL) : site officiel hollandais en matière de cybersécurité. Voir notamment la campagne de sensibilisation Cyber Save Yourself.

NCSC (UK) : site officiel anglais en matière de cybersécurité. Outre de nombreuses guidances, ce site produit notamment des rapports hebdomadaires concernant les menaces rencontrées.

NIST : (National Institute of Standard and Techologies) : site américain proposant de nombreuses publications, workshops et webinars.

SPF Economie : du nom de domaine au manuel de cybersécurité, en passant par les assurances le SPF Economie accompagne les PME dans la mise en œuvre de leur stratégie numérique.

UCM : réalise des enquêtes et suit les enjeux liés à la cybersécurité pour les PME.

UNIZO

En fonction de la région dans laquelle vous habitez, n'oubliez pas de contacter l'agence pour le soutien aux entreprises qui vous concerne. Votre agence pourra également vous donner de précieux conseils notamment en matière de financement.

© Photon_Photo - Fotolia.com

8. Principaux standards

Pour en savoir plus sur les différents standards, vous pouvez consulter le rapport Information security and privacy standards for SMEs de l'ENISA.

8.1. Sécurité de l'information

ISO/IEC 27001: 2013 Information security management systems – Requirements

ISO/IEC 27002:2013 Code of practice for information security controls

ISO/IEC 27003:2010 Information security management system implementation guidance

ISO/IEC 27004:2009 Information security management – Measurement

ISO/IEC 27013:2012 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014:2013 Governance of information security

ISO/IEC TR 27016:2014 Information security management - Organisational economics

ISO/IEC 27032:2012 Guidelines for information security

ISO/IEC 27033-1:2009 Network security - Part 1: Overview and concepts

ISO/IEC 27033-2:2012 Network security - Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033-3:2010 Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

ISO/IEC 27033-4:2014 Network security - Part 4: Securing communications between networks using security gateways

ISO/IEC 27033-5:2013 Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27034-1:2011 Application security - Part 1: Overview and concepts

ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)

ISO/IEC 27040:2015 Storage security

CSA Cloud Controls Matrix

BSI PAS 555:2013 Cyber security risk. Governance and management.

PCI Data Security Standard

ISF The Standard of Good Practice for Information Security

UK Gov. Security policy framework

UK Gov. Cyber essentials scheme

ETSI GS ISI 001 Part 1: A full set of operational indicators for organisations to use to benchmark their security posture

ETSI TR 103 305 Critical Security Controls for Effective Cyber Defence

BSI 100-1 Information Security Management Systems (ISMS)

BSI 100-2: IT-Grundschutz Methodology

8.2. Gestion des risques

ISO/TR 31004:2013 Risk management - Guidance for the implementation of ISO 31000

ISO/IEC 27005:2011 Information security risk management

ISO/IEC 31000 Risk management - Risk assessment techniques

IEC 31010:2009 Risk management - Risk assessment techniques

BSI BIP 0076 Information Security risk management (Handbook for ISO/IEC 27001)

BSI 100-3 : Risk Analysis based on IT - Grundschutz

8.3. Business Continuity Plan

ISO 22301:2012 Business continuity management systems – Requirements [3]

ISO 22313:2012 Business continuity management systems – Guidance

ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity

100-4: Business Continuity Management

8.4. Protection des données à caractère personnel

ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 29100:2011 Privacy framework

ISO/IEC 29101:2013 Privacy architecture framework

BSI BS 10012:2009 Data protection. Specification for a personal information management system

CEN CWA 16113:2010 Personal Data Protection Good Practices

8.5. Incident Management Plan

ISO/PAS 22399:2007 Societal security - Guideline for incident preparedness and operational continuity management

ISO/IEC 27035:2011 Information security incident management

ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence

8.6. Relations avec les tiers

ISO/IEC 27036-1:2014 Information security for supplier relationships - Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information security for supplier relationships - Part 2: Requirements

ISO/IEC 27036-3:2013 Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

8.7. Standards spécifiques (sectoriels)

ISO/TR 13569:2005 - Financial services - Information security guidelines [Financial Services]

ISO/IEC TR 27015:2012 - Information security management guidelines for financial services [Financial Services]

ISO/IEC TR 27019:2013 - Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry [Energy]

ISO 27799:2008 - Information security management in health using ISO/IEC 27002 [Healthcare]

ISO 22307:2008 Financial services - Privacy impact assessment [Financial Services].

economie
SPF Economie, P.M.E., Classes moyennes et Energie

Rue du Progrès 50
1210 Bruxelles
N° d'entreprise : 0314.595.348
https://economie.fgov.be