Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET DE LA ZONE DE DÉFENSE ET DE SÉCURITÉ EST

Direction régionale de l'alimentation, de l'agriculture et de la forêt

23 juillet 2018

Les activités économiques face aux enjeux de cybersécurité

Les systèmes de communication et de production de l'entreprise intègrent de plus en plus, à tous les niveaux, des ressources numériques. Ces ressources sont susceptibles d'être exposées à des attaques malveillantes.

Les conséquences de cyberattaques peuvent être lourdes : l'entreprise doit intégrer la nécessité de **mesures de sécurité** visant à limiter sa vulnérabilité.

Comme tous les acteurs administratifs, économiques, associatifs,..., les entreprises des secteurs agricoles et agro-alimentaires sont concernées. La présente fiche poursuit l'objectif d'un relais de sensibilisation sur les enjeux de cybersécurité. Elle ne préjuge pas des informations plus détaillées accessibles selon d'autres canaux et donne, à ce titre, quelques liens utiles.

✓ De quelles menaces parle-t-on ?

Les attaques de mai et juin 2017 par *Wannacry* et *NotPetya* ont fortement marqué les esprits en raison de la multiplicité des victimes, de l'ampleur de leur propagation et des dommages causés au niveau mondial. Elles n'étaient toutefois que l'expression d'une cybermenace qui **prend des formes diverses** et **évolue en permanence**.

Parmi les menaces les plus courantes ces dernières années dans le cyberespace, on peut citer :

- les attaques en déni de service (DDoS), qui visent à rendre indisponible un service en ligne ;
- le défaçage (ou défiguration) de site internet, par lequel le contenu initial du site se trouve modifié ;
- le *Phishing* (ou hameçonnage), qui consiste à adresser un courriel d'apparence légitime pour obtenir de son destinataire qu'il transmette ses coordonnées bancaires ou ses identifiants de connexion ;
- les rançongiciels, dont relevait notamment *Wannacry*, par lesquels les fichiers de l'ordinateur sont chiffrés (cryptés) en vue d'obtenir le versement d'une rançon.

D'autres types de menaces existent, dont les attaques ciblées (APT), furtives et qui peuvent parfois perdurer des années sans être détectées, ou encore les escroqueries dites « aux faux ordres de virement » (FOVI), qui mobilisent à la fois la voie numérique et des techniques d'ingénierie sociale (manipulation des personnes).

Les objectifs poursuivis sont multiples : destruction ou vol de données, espionnage, escroquerie, sabotage, atteinte à l'image de l'entreprise, propagande, etc.

Pour en savoir plus :
Rapport sur l'état de la menace liée au numérique en 2018 : https://www.interieur.gouv.fr/fr/Espace-presse/Les-communiques/Etat-de-la-menace-liee-au-numerique-en-2018/

✓ Agir pour sa sécurité

Assurer sa cybersécurité n'implique pas nécessairement de mobiliser des compétences avancées, des technologies « de pointe » et d'engager des dépenses hors de portée.

Parfois, les acteurs économiques et en particulier les petites et moyennes entreprises se sentent impuissants du fait d'appréhensions liées à la complexité et au coût supposés de la cybersécurité. Pourtant, il s'agit d'abord de prendre des **précautions « de bon sens »**, dont certaines sont communes à toutes les activités et d'autres seront plus spécifiques aux risques propres à l'entreprise.

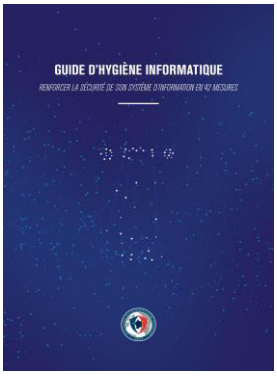
Au plan méthodologique, en effet, il convient d'identifier les **vulnérabilités de l'entreprise**, dont la connaissance s'acquiert par une réflexion sur le niveau de sensibilité des données aux plans stratégique et des enjeux de fonctionnement, la nature des équipements et des logiciels informatiques, les interfaces humaines (personnels, sous-traitants, stagiaires,...) du système d'information.

Cette analyse constitue alors le socle sur lequel peut être définie une réponse adaptée et proportionnée aux risques pouvant fragiliser l'entreprise.

✓ Les précautions élémentaires

Les premières précautions à prendre relèvent d'une application commune à toutes les activités. A titre indicatif, les principales d'entre elles sont les suivantes.

➢ *La sensibilisation des personnels*



Chaque membre du personnel est un maillon du système d'information : lorsqu'il utilise l'ordinateur, le smartphone ou la tablette mis à sa disposition par l'entreprise, tout agent interagit avec le système d'information. Le personnel de l'entreprise doit être sensibilisé aux enjeux et précautions élémentaires de cybersécurité (mesures dites « **d'hygiène informatique** »).

Pour en savoir plus :
Guide d'hygiène informatique (ANSSI) :
https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique
Guide des bonnes pratiques de l'informatique pour les petites et moyennes entreprises (CPME/ANSSI) :
https://www.ssi.gouv.fr/guide/guide-des-bonnes-pratiques-de-linformatique/
« Flash Ingérence » de la direction générale de la sécurité intérieure : https://www.entreprises.gouv.fr/information-strategique-sisse/flash-ingerence

➢ ***La gestion des droits d'accès et des mots de passe***

La gestion des droits, tant physiques qu'informatiques, doit être adaptée à la situation de l'entreprise et aux fonctions de chacun. Des règles claires de gestion des droits d'accès doivent donc être mises en place. Pour éviter qu'ils ne soient facilement usurpés, les mots de passe doivent être robustes, personnels, d'usage unique pour chaque application et régulièrement changés.

➢ ***Les mises à jour logicielles***

Tous les logiciels peuvent comporter des vulnérabilités non identifiées. Lorsque la connaissance s'en trouve acquise, ces vulnérabilités sont corrigées au moyen de « patchs » de sécurité. Il convient de veiller à procéder aux mises à jour logicielles des ordinateurs, smartphones,…

➢ ***La séparation des usages***

La vulnérabilité de l'entreprise est accrue si les personnels utilisent de manière indifférenciée leurs équipements numériques (ordinateurs, smartphones, clés USB,…) à la fois pour des usages professionnels et personnels, voire connectent des équipements personnels directement sur le réseau informatique de l'entreprise. La séparation des usages est un élément essentiel de cybersécurité.

➢ ***La sauvegarde des données***

Certaines attaques informatiques peuvent se traduire par une **perte irrémédiable de données**. En cas d'attaque par un rançongiciel par exemple, payer la rançon ne garantirait aucunement de récupérer ses fichiers. Une sauvegarde régulière des données, sur support dédié disjoint du réseau, est indispensable pour assurer sa **résilience** face au risque de cyberattaques.

➢ ***Les outils de protection***

Pour la sécurité des systèmes, équipements et données numériques de l'entreprise, il est recommandé d'utiliser :

- des logiciels antivirus et pare-feux performants ;
- des solutions de chiffrement des matériels mobiles (ordinateurs portables, smartphones, tablettes) pour les personnels occupant des fonctions sensibles, afin de préserver les données en cas de perte ou de vol ;
- des filtres de confidentialité d'écran, en cas de déplacements réguliers par le train ou l'avion.

➢ ***L'informatique de production***

Le numérique n'est pas présent que sur les fonctions administratives, de gestion ou de communication de l'entreprise. Il est nécessaire d'intégrer dans la réflexion, s'il y a lieu, les éventuels systèmes d'acquisition et de contrôle de données (SCADA) utilisés pour la continuité et le bon fonctionnement des processus industriels.

➢ ***Les risques liés à l'externalisation***

L'entreprise peut choisir de confier à un tiers tout ou partie de la gestion de son système d'information (infogérance). Externalisation et sécurité des systèmes d'information ne doivent pas être opposées, mais imposent d'en évaluer et d'en maîtriser les risques.

> ***Pour en savoir plus :***
> Guide « Maîtriser les risques de l'infogérance » (ANSSI) :
> https://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/

➢ ***Les réseaux sociaux***

Les réseaux sociaux peuvent être des points d'entrée pour la collecte d'informations d'ingénierie sociale nécessaires à la conduite de certaines cyberattaques. La sensibilisation des personnels doit intégrer une incitation à faire preuve de la discrétion nécessaire, sur les réseaux sociaux où ils sont inscrits, concernant leurs activités professionnelles et toute information sensible liée à l'entreprise.

✓ Que faire en cas de cyberattaque ?

En cas de cyberattaque, il est recommandé de recourir au dispositif d'aide aux victimes **cybermalveillance.gouv.fr** (https://www.cybermalveillance.gouv.fr/) afin d'être mis en relation avec des prestataires d'assistance technique qui pourront intervenir en proximité.

L'entreprise pourra par ailleurs **déposer plainte** auprès de la police nationale ou de la gendarmerie nationale ou adresser un courrier au procureur de la République auprès du tribunal de grande instance compétent.

Nota : Au titre de la prévention des cybermenaces, le site cybermalveillance.gouv.fr tient par ailleurs à la disposition des entreprises un ***kit de sensibilisation****.*

✓ Les outils pour se former

Un cours en ligne (MOOC) de l'ANSSI permet de s'initier ou d'approfondir ses connaissances en cybersécurité : https://secnumacademie.gouv.fr/

✓ Autres liens utiles

- Service d'information du Gouvernement : https://www.gouvernement.fr/risques/risques-cyber

- Agence nationale de la sécurité des systèmes d'information (ANSSI) : https://www.ssi.gouv.fr/entreprise/

- Commission nationale de l'informatique et des libertés (CNIL) : https://www.cnil.fr/professionnel

- Police nationale : https://www.police-nationale.interieur.gouv.fr/Actualites/Dossiers/Cybercrime

- Gendarmerie nationale : https://www.gendarmerie.interieur.gouv.fr/Zooms/Cybercriminalite/

Contact DRAAF :

Mission défense et sécurité de zone Est
Mél : jean-francois.laigre@agriculture.gouv.fr
Tél : 03 55 74 10 82