IESF

SOCIÉTÉ DES INGÉNIEURS ET SCIENTIFIQUES DE FRANCE

LES CAHIERS

Novembre 2020

CYBER-RISQUES : LES BONNES PRATIQUES DES PME POUR Y FAIRE FACE

www.iesf.fr

Cet ouvrage a été réalisé par le Comité Maîtrise des Risques Opérationnels des Ingénieurs et Scientifiques de France (IESF), avec la collaboration des membres actifs du groupe de travail suivants :

Benjamin BLANCHARD	IESF/EDF
Yves CABROLIER	IESF/YCCONSULT
Jean-Luc COCHET	IESF/CNPP/AGREPI
Jean-François de RICHEMONT	IESF/Ingénieur Conseil IPF
Pascal GAVID	IESF/AGREPI
Éric JEANCOLAS	IESF/JCRisc
Didier KECHEMAIR	IESF/NOTITIA
Guy PLANCHETTE	IESF/IMdR
François TÊTE	IESF/CCA/DEVOTEAM

Avec l'aide de Christian COLMANT et de François TROCME, membres respectivement des Comités Numérique et Comité Intelligence Économique et Stratégique d'IESF.

INGÉNIEURS ET SCIENTIFIQUES DE FRANCE (IESF)

La France compte aujourd'hui plus d'un million d'ingénieurs et quelque deux cent mille chercheurs en sciences. Par les associations d'ingénieurs et de diplômés scientifiques qu'il fédère, IESF est l'organe représentatif, reconnu d'utilité publique depuis 1860, de ce corps professionnel qui constitue 4 % de la population active de notre pays.

Parmi les missions d'Ingénieurs et Scientifiques de France figurent notamment la promotion des études scientifiques et techniques, le souci de leur qualité et de leur adéquation au marché de l'emploi ainsi que la valorisation des métiers et des activités qui en sont issues.

À travers ses comités sectoriels, IESF s'attache ainsi à défendre le progrès, à mettre en relief l'innovation et à proposer des solutions pour l'industrie et pour l'entreprise. Notre profession s'inscrit pleinement dans le paysage économique et prend toute sa part dans le redressement national.

SOMMAIRE

AVANT-PROPOS

Depuis sa création, le Comité « Maîtrise des Risques Opérationnels » a toujours orienté ses travaux sur le thème de la sécurité industrielle, thème qui concerne l'ensemble des ingénieurs et leurs organismes de formation. Le Comité souhaite poursuivre dans cette direction, en développant des thèmes d'actualité ayant une incidence directe ou indirecte sur les risques opérationnels des entreprises.

Les grandes entreprises industrielles étant généralement dotées de compétences internes ou externes leur permettant de maîtriser ces sujets, les Cahiers du Comité ont pour objectif d'aider les PME-PMI qui n'ont pas toujours les mêmes capacités internes, car le quotidien empêche souvent le chef d'entreprise de consacrer le temps nécessaire à la maîtrise des vulnérabilités de son entreprise.

Dans ses travaux, le comité cherche à promouvoir une démarche de connaissance des risques opérationnels adaptée à leurs besoins et à leur permettre d'appliquer, dans le cadre de la stratégie de leurs dirigeants, des principes de maîtrise de ces risques.

Dans un précédent cahier n° 4, daté du 24 octobre 2011, ce comité proposait des conseils aux dirigeants de PMI/PME concernant la protection des entreprises face aux fraudes, négligences ou malveillances ; la sécurité des systèmes d'information avait été citée en annexe 5 du fait de l'émergence de ce nouveau risque.

Alors que ce risque était encore sous-estimé en 2013 (aux dires des experts consultés) c'est en janvier 2017 que le rapport ALLIANZ RISK BAROMETER positionnait les incidents « cyber » au 3e rang des préoccupations des dirigeants des entreprises. Il devient dans le rapport suivant, en janvier 2018, le risque n° 1 dans les pays anglo-saxons (USA, UK et Commonwealth) devant le risque de perte d'exploitation et d'interruption de la chaîne logistique, risque pourtant prépondérant dans le monde depuis plus de 5 ans.

Dans cette conjoncture où il est devenu une des préoccupations majeures, ce cahier a été rédigé afin d'actualiser la prise de conscience de chacun et de proposer les bonnes pratiques face au besoin d'améliorer dans les entreprises, mais aussi dans la vie privée, la maîtrise opérationnelle d'un cyber-risque omniprésent.

Ce cahier n° 34 a été élaboré en collaboration avec deux experts issus respectivement du Comité Numérique et du Comité Intelligence Économique et Stratégique de IESF.
En stimulant une prise de conscience des vulnérabilités de votre entreprise face aux cyber-attaques, il vous guidera dans la nécessité d'adopter une démarche d'analyse des risques encourus dans le but vous protéger.

Guy Planchette, Président du Comité Maîtrise des Risques Opérationnels

SYNTHÈSE

La transformation numérique est devenue un élément clé de la croissance des PME/PMI, car elle leur permet de gagner en efficacité et de satisfaire aussi bien ses clients que ses collaborateurs.
Ce serait donc aujourd'hui une erreur stratégique de ne pas saisir ces multiples opportunités de productivité et de développement commercial.
Toutefois, ce déploiement du digital conduit à mettre en place un système d'information de plus en plus décentralisé et étendu à des centaines de services interconnectés par le biais de programmes informatisés, le déploiement de milliers d'IOT (internet pour objet)… Les PME/PMI sont alors confrontées à de nombreux risques liés à la sophistication et la diversité des modes d'attaques, à la mobilité des collaborateurs et des appareils…
Ces aspects négatifs imposent aux entreprises d'adopter une nouvelle approche de la sécurité focalisée en particulier sur les identités, les accès et les données.

Désormais, la sécurité doit être pensée comme un élément dynamique et sans cesse adaptée et ajustée en fonction des contextes. La confiance que vous pouvez accorder est fondamentalement une vulnérabilité dans tout système numérique. Aussi, l'un des principes clés à adopter est de considérer toute délégation comme une prise de risque à limiter en n'attribuant aux appareils et aux personnes que les droits dont ils ont besoin en fonction de ce qu'ils ont à réaliser et au moment où ils doivent le réaliser. Pensez également que votre personnel qui maîtrise plus ou moins bien les potentialités du numérique ne possède peut-être pas les réflexes nécessaires vis-à-vis des e-mails frauduleux de type hameçonnage.

Il est donc important d'évaluer vos risques afin de les traiter correctement dans le but de mettre votre entreprise à l'abri de ces multiples attaques qui prennent des formes de plus en plus sophistiquées.

En insistant sur les facteurs influents, ce cahier a aussi l'objectif de vous alerter et vous sensibiliser sur :
- les attaques venant de l'extérieur, car aucune entreprise n'est à l'abri d'actes de malveillance de la part de concurrents nationaux ou internationaux, d'agressivité de personnes à la recherche de rançons,
- et aussi, les vulnérabilités internes de votre entreprise, car le facteur humain est l'un des points les plus sensibles dans une gestion des risques, que ce soit au niveau de vos services informatiques ou des utilisateurs.

A ce stade, nous avons donc pensé utile de vous éclairer sur les recommandations qui paraissent les plus efficaces, aussi bien pour prévenir le risque d'attaques que pour se protéger et tenter de les maîtriser.

Aussi, dans l'esprit de ce que nous sommes en train de vivre avec la pandémie de la Covid, nous vous proposons d'appliquer, à ces virus du digital, l'ensemble des« gestes barrières » décrits dans ce Cahier.

1. DE LA NÉCESSITÉ D'UNE PRISE DE CONSCIENCE PAR LES PMI/PME

1.1 Préambule

En janvier 2019, la France s'est dotée d'une doctrine militaire offensive[1] dans le cyberespace et a renforcé sa politique de lutte informatique défensive[2] :**« Le cyberespace possède une dynamique qui lui est propre : instantanéité des échanges, diffusion en réseau, massivité de données accessibles à tous, effacement des frontières…Il est aussi un multiplicateur d'efficacité pour peu que l'on dispose des bonnes données et informations, qui sont devenues une ressource critique, au cœur du fonctionnement politique, économique et social des sociétés modernes.** »

Pour les entreprises, ces caractéristiques constituent bien entendu des opportunités, avec l'évolution qui est désormais générale vers la « transformation digitale ». Par exemple, l'utilisation intensive du télétravail durant la période de confinement de 2020 liée à la Covid-19 a bien mis en lumière cet intérêt.

Toutefois, il faut aussi tenir compte de la vulnérabilité de nos systèmes informatisés, car ils peuvent être attaqués si l'on n'y prend garde. En effet les objectifs des attaquants potentiels n'ont pas fondamentalement changé : espionnage, sabotage, manipulation, moyens de chantage ; mais leurs modes opératoires sont sans cesse renouvelés par l'émergence continue de nouvelles technologies numériques. Ainsi, selon le panorama 2019 du cyber-crime (« Panocrim » du CLUSIF[2][3]), **la chaine logistique et les tiers sont apparus au cœur des attaques**. Depuis cette année, les attaques par « rançongiciel » impactant des entreprises et institutions dans le monde entier se sont multipliées. Ces codes malveillants représentent actuellement la menace informatique la plus sérieuse pour ces organisations. L'ANSSI partage, par son rapport « État de la menace rançongicielle à l'encontre des entreprises et institutions [4]», son analyse détaillée de la menace, qui se fonde à la fois sur ses observations, ses échanges et ses activités opérationnelles.
Les années 2019 et 2020 ont aussi été particulièrement marquées par les demandes de « rançongiciel » (voir en annexe 6 les témoignages des PDG de la société ALTRAN et de la PME Cadiou-Industrie).

Aussi est-il indispensable de s'appuyer sur une composante forte de la nécessaire maîtrise des risques.

Pour les entreprises, la cyber-sécurité implique la mise en œuvre de recommandations, outils, dispositifs, concepts, méthodes, formation des personnels, voire recrutements de

[1] https://www.pole-excellence-cyber.org/wp-content/uploads/2019/11/Référentiel-Cyber-V5.0.pdf
[2] https://www.defense.gouv.fr/content/download/551555/9394645/Eléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf

[3] https://www.lemondeinformatique.fr/actualites/lire-panocrim-2019-le-clusif-livre-son-etat-des-lieux-de-la-cybercriminalite-77814.html

[4] https://www.ssi.gouv.fr/actualite/rancongiciels-lanssi-livre-son-analyse-de-la-menace-pour-les-entreprises-et-les-institutions/

profils spécifiques. De ce fait, certaines entreprises la perçoivent comme une contrainte, un domaine réservé à quelques experts, une source de coûts supplémentaires.

Les trois excuses les plus répandues pour ne pas s'occuper de cyber-sécurité sont connues [5] :

- nous ne disposons pas de moyens suffisants ;

- il n'y a rien à voler chez nous ;

- plutôt payer qu'investir avant pour rien.

Pourtant, dans un monde de plus en plus connecté, l'enjeu pour la continuité des activités de l'entreprise justifie d'anticiper la « menace cyber », afin de faire face à des actions d'intelligence économique ou de malveillance. Pour protéger les personnes et les actifs matériels comme immatériels (les données et les systèmes connectés qui assurent leur traitement), les mesures en faveur de la cyber-sécurité visent l'objectif général d'améliorer la **résilience** de l'entreprise. Il s'agit de maintenir la disponibilité, l'intégrité, la continuité des activités, mais aussi, le respect de la confidentialité des données stratégiques ainsi que celles relatives aux collaborateurs.

1.2 Constats et statistiques

Le nombre de cyber-attaques en Europe a progressé de 83% entre 2016 et 2019 selon une étude source de Marsh Europe (détails en annexe 1.1).

En 2020, les attaques continuent et à titre d'exemples, citons les plus récentes ;

- la compagnie aérienne britannique EasyJet révèle dans un communiqué publié mardi 19 mai 2020, avoir été victime d'une cyber-attaque « très sophistiquée » ;

- le 17 juillet 2020, MMA a été victime d'une vaste cyber-attaque nécessitant l'arrêt, à titre conservatoire, de tous les systèmes informatiques ;

- le 1er septembre 2020, le Parlement norvégien annonce avoir été victime d'une attaque informatique « importante » visant à pirater les messageries de nombreux députés et employés.

Selon le Baromètre de la cyber sécurité des entreprises (Sondage Opinion Way pour le Club des Experts de la Sécurité de l'Information et du Numérique, CESIN, Vague 5 – Janvier 2020) :

- près d'une entreprise sur deux se dit inquiète quant à sa capacité à faire face aux cyber-risques (détails en annexe 1.2) ;

- les entreprises, conscientes des risques, sont 91% à mettre en place un programme de cyber-résilience ou à envisager de le faire, soit 12 points de plus qu'en 2018. Elles sont également plus nombreuses à avoir souscrit une cyber-assurance (60% contre 50% en janvier 2019) ;

- le taux d'entreprises déclarant des cyber-attaques est en baisse en 2019 : 65% en ont connu au moins une contre 80% l'année dernière. Les cyber-attaques ont malgré tout un impact sur le business similaire à l'année dernière (57%), provoquant principalement des

[5]Source : Guide 2019-2020 cyber-sécurité Hors-série Solutions Numériques

perturbations de la production. Les grands types d'attaques subies par les entreprises : l'attaque par hameçonnage (79%), et l'arnaque au président (47%). L'usurpation d'identité (35%) et l'infection par un malware (34%) sont les conséquences directes de ces cyber-attaques. La négligence ou l'erreur de manipulation ou de configuration d'un salarié (43%) est le cyber-risque le plus répandu (annexe 1.3) ;

- 89% des entreprises utilisent le « cloud » pour stocker une partie de leurs données, 55% le font avec le « cloud » public. Cet outil de stockage pose cependant des risques, les plus forts étant la non-maîtrise de la chaîne de sous-traitance de l'hébergeur (50%), la difficulté de mener des audits (46%), et la non-maîtrise de l'utilisation du « cloud » par les salariés (46%). Pour pallier ce manque de sécurité, 91% des entreprises estiment que des outils et/ou dispositifs spécifiques doivent être mis en place ce qui interroge sur la pertinence des outils de sécurité proposés par les acteurs du « cloud » ;

- seules 4 entreprises sur 10 se disent préparées en cas de cyber-attaque de grande ampleur (annexe 1.4) ;

- parmi les enjeux de demain pour cyber-sécuriser les entreprises, ceux concernant le budget mais surtout l'humain sont à privilégier. Les salariés sont pourtant sensibilisés aux cyber-risques (74%) mais manquent visiblement d'implication. D'après les Responsables en charge de la Sécurité des Systèmes d'Information (RSSI), seule la moitié des salariés respectent les recommandations. Pour tenter de les mobiliser plus durablement, 77% des entreprises ont mis en place des procédures pour tester l'application des recommandations par les salariés (annexe 1.5) ;

- l'augmentation du budget (50%) est un autre enjeu majeur. La part du budget informatique consacré à la sécurité augmente dans les entreprises, et devrait continuer à augmenter puisque 62% d'entre-elles indiquent vouloir allouer plus de ressources à la cyber-sécurité et 83% souhaitent acquérir de nouvelles solutions techniques (annexe 1.6) ;

- en France, 60% des attaques concernent des PME (Ministère de l'Intérieur, État de la menace liée au numérique en 2017, janvier 2017). Les objets connectés [Internet of Things (IoT)] sont de plus en plus présents, notamment dans les commerces, le petit tertiaire et le résidentiel. Le laboratoire PRADEO a réalisé une étude démontrant que 80 % des applications testées comportent des vulnérabilités. Toutefois, « seulement » 15 % de ces applications seraient totalement vulnérables à la prise de contrôle. Parmi les logiciels malveillants (malwares) les plus couramment utilisés contre les IoT, figure l'attaque « Man-in-the-middle » qui permet de prendre le contrôle de l'objet connecté.

1.3 Importance de la prise de conscience par les PME/PMI

Le bilan de ces constats et statistiques montre que ces entreprises, disposant de peu de moyens d'étude, sont mal préparées à des attaques de grande ampleur et présentent en plus d'importantes vulnérabilités,

Aussi, la prise de conscience de ces fragilités doit conduire à des actions prioritaires afin de conserver la pérennité des entreprises.

Ce cahier a donc le modeste objectif de rassembler en quelques pages un ensemble d'informations et de réflexions utiles aux PME-PMI afin de leur permettre de mettre en place une politique de sécurité informatique adaptée à leurs besoins. Toutefois, ce message peut aussi être utile à de plus grandes entreprises ou organisations telles que les collectivités locales ou hôpitaux, qui ont aussi fait l'objet d'attaques en 2019.

Pour compléter les informations contenues dans ce cahier, vous trouverez quelques recommandations émises par des organismes spécialisés, que vous pourrez consulter en annexe 3.

2. UNE DÉMARCHE D'ANALYSE DE RISQUES

La démarche d'analyse de risques offre la possibilité de se préparer à la survenue d'événements aléatoires et défavorables. Elle permet de :
- définir des mesures de prévention pour diminuer la vraisemblance de ces événements ;
- déterminer des mesures de protection pour en diminuer les conséquences ;
- se poser quelques bonnes questions comme « Est-ce que le risque en vaut la chandelle ? » ou « Dois-je m'assurer contre ce risque ? ».

Cette démarche n'est pas spécifique à une branche. Elle permet d'identifier les vulnérabilités de tout type de structure ou d'activité. Elle est adaptable à tout contexte. Cette démarche implique des analyses systématiques et récurrentes, car les menaces évoluent avec le temps.

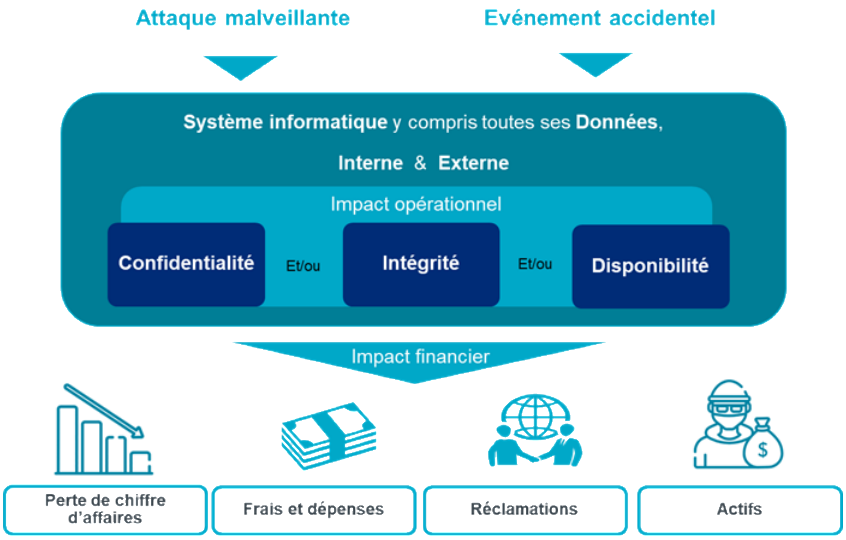
Dans le domaine spécifique des cyber-risques, l'ANSSI préconise la méthode EBIOS Risk Manager[6] qui accompagne les organisations - en intégrant l'ensemble des parties prenantes - pour leur permettre d'identifier et de comprendre les risques numériques qui leur sont propres. Cette analyse vise à définir les mesures de sécurité adaptées à la menace et de mettre en place le cadre de suivi et d'amélioration continue à l'issue d'une analyse de risque partagée au plus haut niveau.
Cette méthode n'est toutefois pas exclusive des méthodes qui assurent la conformité à des règlements européens, comme le RGPD (règlement général sur la protection des données), et à des normes internationales de management de la qualité (ISO 9001), de l'environnement (ISO 14001) et bien sûr de la sécurité de l'information (ISO/CEI 27001).

L'ensemble des parties prenantes comprend, entre autres, tous les donneurs d'ordre avec lesquels les PME sont interconnectées, ainsi que leurs éventuels sous-traitants. Aussi est-il nécessaire d'intégrer la notion d'interdépendance, puisqu'une chaîne ne vaut que par son maillon le plus faible.

De plus, les PME-PMI ne disposent pas toujours de moyens humains et financiers suffisants pour conduire de façon approfondie et régulièrement actualisée de telles analyses de risque. Par exemple, il n'existe pas toujours au sein de l'entreprise un responsable dédié au système d'Information (SI).

Pourtant l'enjeu n'est pas neutre vis-à-vis des assurances à double titre. D'une part, l'assureur prendra certainement en compte le fait que la structure dispose d'un mécanisme organisé de détection et de traitement de ses vulnérabilités. D'autre part, la mise en place d'une gestion de risques efficace réduira la probabilité d'occurrence des événements redoutés ainsi que la gravité des conséquences pour l'entreprise. Parmi les analyses de risques, l'assureur Marsh propose la démarche suivante :

[6] https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/



Pour conduire une démarche d'analyse des risques, il est conseillé d'utiliser les diverses méthodes classiques existantes ou de faire appel à des prestataires. Nombreux sont ceux qui peuvent réaliser de façon structurée de telles analyses de risque adaptées aux enjeux. L'ANSSI recommande de faire appel aux prestataires ayant déjà obtenu des « visas de sécurité délivrés par l'ANSSI[7] ».

Il n'entre pas dans les objectifs du présent document de détailler les méthodes, mais plutôt de donner quelques orientations simples et pragmatiques à l'usage des responsables.

2.1 Hiérarchiser les risques

Comme pour toute analyse de risque, le cas du risque cyber peut être approché en distinguant :

- les vulnérabilités de l'entreprise ;
- la probabilité d'occurrence d'un évènement entraînant une défaillance ;
- l'impact en cas de défaillance avérée.

Sans aller jusqu'à une procédure formalisée complète d'audit des SI de l'entreprise, qui peut parfois se révéler lourde et coûteuse, une démarche interne de prise de conscience de ces différents aspects du risque peut permettre à l'entreprise, grâce à un questionnaire d'autodiagnostic placé en annexe 4, de s'engager sur la voie d'une meilleure prévention.

2-1-1- Vulnérabilité

L'analyse doit couvrir non seulement les aspects techniques, mais aussi les aspects humains et organisationnels.
Une analyse des exigences réglementaires et des engagements contractuels qui s'appliquent à l'entreprise peuvent l'aider dans cette phase.

2-1-2- Probabilité d'occurrence d'un événement entraînant défaillance

Pour estimer cette probabilité d'occurrence, il est souhaitable d'imaginer des scénarios décrivant, à partir d'une dérive ou défaillance, l'ensemble du déroulement potentiel

[7] https://www.ssi.gouv.fr/administration/visa-de-securite/

aboutissant à l'accident. Par exemple, en cas de failles techniques ou humaines, avec quelle probabilité un hacker peut pénétrer le cœur de mon SI, via internet ou hors connectivité.

2-1-3- Impact

Ensuite, il convient de distinguer :

- les impacts internes à l'entreprise ;
- les impacts, potentiellement plus graves, d'une attaque qui utiliserait la structure comme point d'accès vers un de ses donneurs d'ordre.

Dans les deux cas, il est important de hiérarchiser si possible à partir d'éléments quantitatifs, les impacts :

- perte de CA (sur les contrats en cours) ;
- interruption d'activité (totale ou partielle, pendant combien de temps, …) ;
- perte de données (lesquelles, quelle est leur sensibilité, …) ;
- perte de « réputation », donc de CA futur ;
- conséquences juridiques, voire pénales pour les responsables ;
- coûts de gestion de crise, puis de remédiation (d'autant plus élevés que le recours à un prestataire spécialisé n'aura pas été anticipé).

Il est clair que l'analyse d'impact ne peut être conduite qu'en relation avec les donneurs d'ordres. La cartographie du « réseau » des SI interconnectés peut se révéler complexe. Cette complexité supplémentaire peut toutefois constituer un atout, si certaines organisations dans le réseau d'interconnexions en question (grands groupes industriels, collectivités locales, organisations de la sphère publique, …) ont déjà pour leurs propres besoins mené une analyse de risque cyber avec des moyens dépassant ceux accessibles pour la PME-PMI considérée. On est alors typiquement dans le schéma d'une analyse de risque « système » dont les avantages peuvent être collectivement bénéfiques.

2.2 Traiter les risques

Ce sont les mesures à prendre pour limiter le risque, s'en protéger, assurer la remédiation si besoin (plan de continuité d'activité, travail sur la résilience de l'activité, …)

Parmi les actions simples à mettre en œuvre (qui relèvent de « l'hygiène informatique » pour laquelle l'ANSSI fournit des guides précis) :

- sensibilisation formation régulière des personnels, notamment à séparer les usages personnels des usages professionnels ;
- limitation au strict nécessaire des droits d'accès (gestion des « privilèges ») aux différentes fonctions du SI ;
- mise à jour régulière des versions des logiciels ;
- procédure formalisée de renouvellement périodique des mots de passe ;
- procédure formalisée de sauvegarde des données ;
- recours éventuel en amont à un prestataire d'alerte et de gestion de crise.

2.3 Tirer les leçons des attaques ou des incidents

La menace cyber évolue vite et en permanence. Se protéger dans une logique de forteresse imprenable serait illusoire et les moyens mis en œuvre seraient sans doute dépassés techniquement dès le jour de leur déploiement. Le cyberespace est en effet un espace dans

lequel, à ce jour, l'avantage est toujours à l'attaque. C'est une logique de « progrès continu » associant les composantes techniques, humaines, et organisationnelles qui doit guider la démarche.

On observe ainsi deux tendances dans des attaques récentes :

- une préparation de plus en plus longue ;
- une attaque de plus en plus fréquente des systèmes instrumentés de sécurité (SIS) ou systèmes de contrôle industriel (ICS).

Ainsi, l'un des moyens les plus efficaces pour renforcer la vigilance et la protection des organisations consiste à tirer les leçons des attaques ou tentatives d'attaques passées.
Il est possible d'avoir recours là encore à un prestataire spécialisé (offres sur le marché de type SOC). Ces moyens, certes efficaces, mais assez lourds et coûteux, peuvent s'avérer hors de portée d'une PME/PMI prise isolément. Plusieurs initiatives en cours tentent de proposer des services mutualisés, à coût réduit, (voir annexe 3).

2.4 Analyser les exigences réglementaires ou les engagements contractuels

Initialement, c'est la *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés qui a initié le droit et la sécurité informatique.*

En 2016, la loi pour la modernisation de la justice, a introduit à l'article 43ter de la loi informatique et libertés de 1978, la possibilité d'une action de groupe en matière de protection des données pour faire cesser les manquements aux règles, etc.

Le 25 mai 2018, le régime de responsabilité issu du règlement européen sur la protection des données personnelles (RGPD) est entré en vigueur. L'ensemble de ces réglementations confirme les changements importants en matière de cyber sécurité.

Les autorités publiques européennes fixent les fondements d'une nouvelle réglementation en matière de cyber protection. Le 12 mars, le Parlement européen, puis le 7 juin 2019 le Conseil de l'Union européenne ont adopté le règlement européen « CybersecurityAct ». Le double objectif est de donner mandat permanent à l'Agence européenne pour la cyber-sécurité, et à définir un cadre européen de certification de cyber-sécurité, pour renforcer la sécurité du marché unique numérique européen.

L'entreprise a donc l'obligation de **sécuriser** ses systèmes d'information par :

1. **la protection et la gestion des données concernant la clientèle ;**
2. **la gestion de toutes les données confidentielles des collaborateurs ;**
3. **un rappel du droit des bases de données ;**
4. **des mesures techniques appropriées par une traçabilité des mesures informatique ;**
5. **la gestion des procédures d'habilitation à intégrer ou modifier les données.**

2.5 Tenir compte du niveau de maîtrise de l'exploitant

Grâce à la réflexion proposée parle questionnaire d'auto diagnostic (annexe 4), le responsable de PME-PMI peut effectuer (ou faire effectuer) une première évaluation de la situation de son entreprise vis-à-vis des cyber risques.

2.6 Formaliser le résultat de l'analyse des risques

Le résultat de l'analyse du risque cyber doit être retranscrit en fonction d'une échelle du niveau de sûreté attendu.

Une échelle de sûreté sur trois niveaux[8] permet une approche pragmatique de la sécurité opérationnelle d'un SI industriel face au risque cyber :

1. **Niveau de sécurité faible :** état dans lequel le SI présente de nombreuses vulnérabilités connues, simples à exploiter et permettant à un attaquant de prendre très facilement le contrôle total du SI. Des attaques dans cette situation peuvent avoir des conséquences catastrophiques: destruction irréversible d'information, pillage en profondeur du patrimoine informationnel, perturbation durable des opérations.

2. **Niveau de sécurité d'élémentaire à moyen :** Permet au SI de résister aux attaques les plus triviales. Ces mesures contribuent à diminuer sensiblement la surface d'exposition aux menaces. Mais une personne mal intentionnée pourra cependant trouver une brèche de sécurité et concevoir une attaque ciblée. L'effort pour passer du niveau 1 au niveau 2 est très important :
   - les accès à Internet ont été rationalisés, centralisés et contrôlés ;
   - les systèmes les plus exposés à Internet ont été signalés et sécurisés ;
   - les postes de travail ont aussi été sécurisés, ou sont en passe de l'être ;
   - il n'y a plus de mots de passe triviaux dans les équipements les plus sensibles ;
   - il existe un début de supervision de la sécurité se limitant à une surveillance des antivirus et occasionnellement des journaux du pare-feu ;
   - les comptes de personnes ayant quitté depuis longtemps l'entreprise sont supprimés, l'accès au groupe « administrateur du domaine » est rigoureusement limité.

3. **Niveau de sécurité d'important à très important, sécurité maîtrisée :** peut être atteint après les précédentes mesures prises. Pour compromettre le SI, l'attaquant doit maintenant concevoir des attaques bien plus complexes. Mais grâce aux dispositifs de surveillance et de gestion d'incidents, de telles attaques seront détectées et leurs impacts seront limités. Cependant, certains facteurs chroniques demeurent :
   - la complexité actuelle des SI rend impossible une sécurisation complète ;
   - même si les identités sont très bien gérées, il est impossible d'avoir la certitude absolue qu'aucun compte indûment privilégié n'est passé à travers les mailles ;
   - certains anciens systèmes ou applications échappent à la sécurité, et les compétences pour les maintenir sont obsolètes ;
   - certaines personnes ou fonctions de l'entreprise peuvent encore argumenter et « résister » à appliquer les bonnes pratiques.

[8] Source : « Sécurité Opérationnelle, Conseils pratiques pour sécuriser le SI », Alexandre Fernandez-Toro, Eyrolles

3. LES FACTEURS INFLUENTS

Vis-à-vis des cyber-risques, de nombreux facteurs de contexte, technologiques, humains et organisationnels, vont jouer un rôle positif ou négatif.

3.1 Facteurs de contexte

Périmètre des activités de l'entreprise, échanges avec clients et partenaires

Aucune entreprise n'est à l'abri d'actes de malveillance de la part de concurrents nationaux ou internationaux. Les PME sont concernées. Toute entreprise, qu'elle offre des services et des prestations basées sur l'usage de l'information (matériels connectés, logiciels, etc.) ou pas, s'expose envers ses **clients**, dans le cas où sa prestation ou sa négligence est à l'origine d'une cyber-attaque qu'elle aura favorisée. Les conditions générales de ventes doivent prescrire a minima un standard de bonnes pratiques.

Les échanges avec les **partenaires (fournisseurs, clients, financeurs, …)** peuvent nécessiter des connexions informatiques et des échanges de données. Ces liens sont une source de risque, si le partenaire n'est pas lui-même fiable dans le domaine des cyber-risques ou s'il ne respecte pas la réglementation afférente.

Risque d'image

Une entreprise qui ne saura pas gérer ou limiter les conséquences d'une cyber-attaque pourra voir son image durablement impactée et, surtout, perdra la confiance de ses partenaires et de ses clients.

Les entreprises négligentes en cyber sécurité pourront se voir refuser l'accès :

- aux procédures de marchés publics dématérialisés ;
- à des plateformes digitales avec maintien de la confidentialité (chiffrement) ;
- à la demande de dématérialisation des marchés et l'obtention de signature électronique (non-répudiation).

Choix budgétaires

Les choix économiques (dépenses consenties) opérés par l'entreprise vont avoir un impact sur le niveau des risques de l'entreprise (ressources humaines, formation des collaborateurs, communication interne sur les risques, qualité des matériels et des logiciels, surveillance des réseaux et de matériels, niveau des prestataires dans le domaine de l'information, outils de contrôle, de maintenance et de correction des systèmes d'information.

L'entreprise peut souscrire à une assurance contre les cyber-risques qui lui permettra, selon le niveau de contrat, d'en supporter les conséquences financières. Dans le cadre de ces contrats, les assureurs proposent des prestations de conseil pouvant aller jusqu'aux tests d'évaluation de la résistance des systèmes informatiques vis-à-vis des cyber-attaques.

3.2 Facteurs technologiques

Choix des matériels

Les évolutions technologiques sont très rapides. Mais le choix initial de l'architecture des systèmes et des technologies (matériels et logiciels)et leur maintenance sont essentiels. Il doit refléter les justes besoins de l'entreprise, sans céder aux facilités offertes par des services non indispensables, qui peuvent être autant de sources de vulnérabilités : télé-opérabilité, télémaintenance, réseaux sans fil, etc.

Les matériels nomades sont évidemment particulièrement vulnérables aux risques de malveillance (vol de matériel, captation des données, introduction de virus, etc.). C'est, là aussi, un choix de l'entreprise qui doit mettre en place les moyens adaptés à l'enjeu : données cryptés, ports USB désactivés, fonction « bluetooth » désactivée, lecteurs de disques désactivés, liaison Réseau Privé Virtuel (VPN), etc.

L'usage des « Bring Your Own Device » (BYOD) se répand pour des raisons de coût, de performance des matériels personnels, de « porosité » croissante entre vie professionnelle et vie privée (télétravail, …). Ils doivent être protégés spécifiquement pour éviter de constituer des portes d'entrées dans le système de l'entreprise[9].Sur ce point du nomadisme, l'ANSSI a également publié des recommandations spécifiques[10].

Architecture du système : fermé ? ouvert ?

Un grand nombre d'entreprises ont développé un réseau interne (intranet) lui-même connecté au réseau externe (extranet). Le réseau interne offre une relative protection vis-à-vis des attaques externes, pour autant qu'il soit suffisamment bien surveillé et protégé. Pour protéger des installations et/ou des informations très sensibles, il est recommandé que ce réseau interne n'ait aucune connexion **physique** avec le réseau externe. Les échanges d'informations avec l'extérieur, doivent se faire par un protocole de transfert via des appareils indépendants du réseau interne. Ceci entraine des contraintes élevées au niveau du fonctionnement.

A contrario, on assiste aujourd'hui à un développement du principe de partage de ressources (mémoires, capacités de calcul, banques de données) via des « clouds » externes. Certains experts considèrent que le recours au « Cloud » est une option pour améliorer la résilience face aux attaques cyber. A l'heure actuelle, il n'existe pas de solutions pleinement satisfaisantes. Une logique plus « ouverte » est sans doute en effet mieux adaptée à un « progrès continu » de la cyber-sécurité des systèmes. La question centrale n'est alors plus d'éviter l'attaque, mais de garantir la continuité de service, éventuellement en mode dégradé, en cas d'attaque et d'être capable de restaurer l'ensemble des fonctionnalités au plus vite. C'est une stratégie de « résilience ».

In fine, le critère fondamental est la confiance qui peut être accordée à l'opérateur du « Cloud » qui est à étudier cas par cas. A chaque entreprise de mesurer les avantages et les inconvénients (risques) de cet usage.

Surveillance des réseaux

[9] https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
[10] https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-

Quelle que soit l'architecture technique choisie pour le système, une surveillance du fonctionnement de ces réseaux de circulation d'informations est incontournable.

Tout d'abord, si les matériels (les divers ordinateurs ou « serveurs » de l'entreprise) sont installés au sein de l'entreprise, ils nécessitent une protection physique contre diverses atteintes d'intégrité comme l'inondation, l'incendie, les pannes d'énergie, les actes de malveillance. Le recours croissant à des appareils « nomades » (« smartphones », ordinateurs portables, tablettes, …) ne dispense pas de précautions dans le même esprit (face au vol de matériels par exemple). En conséquence, la protection et le maintien en conditions opérationnelles de son parc de matériels exige de l'entreprise une organisation et un suivi rigoureux, qui contribuent à réduire les risques de dégradations physiques, mais aussi d'obsolescence (en particulier des logiciels).

L'organisation par l'entreprise de ses systèmes d'information (SI) peut alors lui permettre de disposer d'outils pour mieux surveiller les flux d'informations liés à son activité sur les réseaux internes ou externes : hiérarchisation de sensibilité des données, archivage systématisé et d'accès rapide, traçabilité des échanges, détection de signaux faibles via le repérage d'échanges « atypiques », etc. C'est une conséquence positive non négligeable de la mise en place d'une démarche globale de progrès pour la maîtrise des risques cyber.

Dans le cas où les besoins en SI sont exploités par des opérateurs de réseaux et les serveurs regroupés dans des « data centers » :

- les infrastructures sont de véritables bunkers exploités 24h/24 et doivent être particulièrement surveillés, ce qui nécessite des moyens logistiques et énergétiques considérables ;

- le traitement par les opérateurs de réseaux des flux d'informations implique un « pouvoir de surveillance » qui rejoint celui des États (ce dernier étant utilisé, on l'espère, dans les limites de leur légitimité démocratique), ce qui n'est pas sans poser quelques questions, s'il est laissé aux mains d'intérêts purement commerciaux.

Numérisation de procédés industriels

La numérisation de procédés industriels peut apporter souplesse et performance, mais elle augmente aussi les risques :

- de prise de contrôle malveillante si le système numérique est connecté avec ou sans fil ;

- de complexification des procédures de conduite numérique, à maîtriser par les opérateurs du procédé, habitués à une conduite traditionnelle ;

- de possibilité de panne informatique du système numérique de pilotage, hors du domaine de compétences des équipes habituelles de maintenance du procédé.

Bien entendu, ces risques peuvent être maîtrisés, à condition de prendre en compte dès la conception du système, les choix technologiques (voir précédemment), et surtout la formation du personnel. Prévoir, si cela est réaliste, la possibilité de reprendre la conduite du procédé par des moyens traditionnels en cas de panne du système numérique. Pour ce faire, des procédures testées périodiquement doivent être prévues.

Enfin, un plan de continuité d'activité doit permettre de limiter les conséquences d'un black-out ou d'une panne majeure du système numérique.

Les risques sont particulièrement grands lorsque les défaillances des processus ainsi numérisés peuvent provoquer des accidents industriels ou lorsque ces processus assurent eux-mêmes des fonctions de sécurité.

3.3 Facteurs humains et organisationnels

Les facteurs humains jouent un rôle essentiel dans la maîtrise des risques au sein des entreprises, comme nous l'avons rappelé dans le cahier n°28.

On pourrait même être tenté de dire que le facteur humain est à l'origine de la quasi-totalité des risques parle manque de surveillance ou de vigilance dans les processus industriels ou dans la conception et la réalisation de programmes informatiques.

La détection du risque humain est à la fois l'un des points sensibles dans une gestion des risques mais aussi l'un des points prioritaires. Le domaine cyber n'échappe pas à la règle. Les pirates informatiques ont recours au renseignement passif voire à la manipulation, plus simples à mettre en œuvre qu'une cyber-attaque sur un système d'information protégé.

Vis-à-vis de l'informatique en général, deux grandes familles de personnels sont à considérer dans l'entreprise : les services informatiques et les utilisateurs. Selon la taille de l'entreprise, les informaticiens peuvent être des salariés internes à celle-ci ou des prestataires externes qui, selon les cas, gèrent une part plus ou moins complète de services informatiques. Aucune de ces formules n'élimine complètement les risques.

Services informatiques internes

Les informaticiens (au sens large) constituent une population qui possède les compétences nécessaires pour concevoir, programmer et exploiter les systèmes d'information (structure, matériels, logiciels). Cette population est en quelque sorte au service des autres entités de l'entreprise pour leur permettre de développer les activités liées à son cœur de métier. Cette remarque est bien entendu très générale et ne s'applique pas aux entreprises évoluant dans le domaine spécifique de l'informatique.

Les informaticiens salariés de l'entreprise peuvent se sentir très concernés par l'avenir de l'entreprise et avoir à cœur de mettre en œuvre les meilleures solutions pour maîtriser ses cyber-risques. De plus, après une certaine durée de présence dans l'entreprise, ils en connaissent mieux les besoins, les contraintes, les forces et les faiblesses. Il faut faire la distinction entre le secteur tertiaire (ou l'administration des secteurs industriels), pour lequel les systèmes et les outils informatiques, en dehors des applicatifs spécifiques, sont plutôt similaires d'une entreprise à l'autre, et la partie production du secteur industriel qui utilise des technologies variées, parfois complexes, voire disparates (voire obsolètes…). Pour ce secteur, les compétences informatiques nécessaires rendent pratiquement indispensable une intégration du service dans l'entreprise.

Le niveau de qualité, de compétence et de confiance de cette entité dépendra aussi des moyens que l'entreprise a choisi d'y consacrer. A ce titre, les nouvelles menaces cyber nécessitent un approfondissement des connaissances des informaticiens dans ce domaine. Le recrutement de salariés informaticiens représente donc aujourd'hui un enjeu crucial, qui justifierait le recours à des recruteurs spécialisés.

L'inconvénient majeur de ces équipes internes en matière de risques est la contrepartie de ses avantages. En matière informatique, dans un monde très rapidement évolutif, l'arrivée de sources et d'idées nouvelles en provenance de l'extérieur de la structure permet de disposer plus facilement d'une technologie évolutive et peut être plus performante pour les besoins de la structure.

Prestataires externes

Un prestataire externe à l'entreprise peut apporter une compétence et une expertise issues de multiples expériences dans d'autres entreprises. Il peut faire partie d'un groupe d'envergure nationale ou internationale possédant des moyens de formation, de sélection des compétences et des moyens logistiques et informatiques que ne pourrait pas s'offrir l'entreprise cliente.

L'inconvénient, pour l'entreprise cliente, est le risque de dépendance vis-à-vis de ce prestataire qui ne peut souvent pas être remplacé « au pied levé ». Il ne faut pas négliger, non plus, le risque de fuites d'informations sensibles concernant notamment l'organisation de l'entreprise, ses données clients et ses secrets de fabrication. L'entreprise doit donc pouvoir instaurer des contrôles périodiques avec le prestataire afin de s'assurer de la bonne réalisation de sa mission.

Parmi les critères de choix d'un prestataire, il sera bien entendu indispensable de considérer ses compétences dans le domaine des cyber-risques. Cette prestation particulièrement sensible doit faire l'objet d'une contractualisation précise et sans ambigüité, permettant à l'entreprise cliente d'utiliser des moyens de recours en cas de problème. Le contrôle interne des prestations fournies, nécessite la présence, au sein de l'entreprise cliente, d'un service compétent. A défaut, une tierce partie devrait être requise.

Autres personnels

Les utilisateurs de l'informatique, qui représentent la quasi-totalité du reste de l'entreprise, ont en principe à leur disposition des outils (matériels et logiciels) qu'ils maîtrisent plus ou moins et pour lesquels leurs niveaux d'accès sont souvent restreints. Leur formation aux outils informatiques est évidemment très hétérogène selon les populations, leurs métiers, leur âge et leur intérêt pour ces questions.

L'entreprise ne peut donc pas ignorer cette question et doit connaître, pour chaque salarié, les besoins en connaissances informatiques, ne serait-ce que pour utiliser/exploiter correctement les outils nécessaires aux postes de travail. La bonne adéquation des compétences des salariés vis-à-vis de leurs outils de travail est un facteur essentiel en matière de maîtrise des risques, en limitant les risques d'erreur, voire d'accident, et en permettant aux salariés de travailler de façon optimale et satisfaisante pour leurs attentes personnelles.

Le niveau d'accès des utilisateurs des moyens informatiques doit être adapté à leur strict besoin, ce qui passe, notamment, par une définition claire des postes de travail. L'entreprise doit sensibiliser le personnel vis-à-vis des cyber-risques pour lui permettre de comprendre son rôle dans ce domaine, savoir appliquer les règles de sécurité et admettre les nouvelles contraintes que ces règles peuvent avoir sur le travail quotidien. Le personnel doit également être informé des diverses formes de cyber-attaques et éventuellement leur parade, afin de ne pas contribuer à l'extension de la menace au sein de l'entreprise et remonter l'information au plus vite vers les services compétents pour la gérer.

Un accompagnement peut être nécessaire pour certaines catégories de personnels dont les postes de travail sont fortement impactés par la révolution numérique. Comme l'ANSSI, on peut ici parler « d'hygiène informatique », et mentionner quelques points clé : protection physique des bureaux où se trouvent des postes informatiques « sensibles » (et en tout premier lieu ceux de la Direction Générale de l'entreprise …), gestion des mots de passe par chacun (et pas seulement sur les postes informatiques au bureau : certaines attaques sont passées par les postes personnels et des connexions VPN avec le bureau …), et bien entendu, actions régulières de sensibilisation auprès de l'ensemble des personnels. Ces points seront détaillés au chapitre 3 « Les recommandations ».

Procédures et facteurs organisationnels

Le choix et la manière d'exploiter des systèmes informatisés/automatisés aura une incidence importante sur le niveau de vulnérabilité de l'entreprise.

Les facteurs organisationnels contribuent à une grande majorité des risques. Mais certains d'entre eux peuvent être facilement traités et pour un coût relativement faible. En effet, l'un des aspects assez fréquents réside dans la gestion des habilitations qui constitue souvent l'un des points faibles des organisations. A titre d'exemple, il est souvent constaté que des habilitations sont conservées alors qu'elles n'ont plus lieu d'être.

Cette gestion en matière d'habilitation des personnes et de leur niveau d'autorisation doit donc être actualisée en permanence sous peine de rendre inopérant l'efficacité des procédures d'accès au niveau du système d'information. En ce domaine, la réactivité est une condition de l'efficacité.

Le niveau d'accès des systèmes doit être adapté en fonction des besoins et des compétences des différents utilisateurs.

De manière générale, toutes les procédures relatives à l'informatique et à ses usages, doivent être connues de tous ceux qui ont à les mettre en œuvre, puis testées régulièrement et mises à jour. Tout écart par rapport à ces principes doit être détecté, signalé et une suite doit être donnée.

Sauvegardes

Tout système numérique est représenté par un ensemble de matériels, de logiciels et de données (dont font aussi partie les logiciels). Ces logiciels et données ont la particularité de pouvoir être dupliqués autant de fois que nécessaire afin d'assurer leur sauvegarde.

La sauvegarde est donc un élément prioritaire de la sécurité informatique. Toutes les précautions doivent prises pour garantir fiabilité, confidentialité et disponibilité des sauvegardes. On peut, notamment, citer les conditions suivantes :

- mise à jour régulière des sauvegardes selon une fréquence (planification) adaptée aux besoins ;
- test de reprise régulier des sauvegardes pour vérifier leur efficacité ;
- protection physique des sauvegardes (cf « facteurs technologiques ») ;
- protection des sauvegardes contre les cyber-attaques ;
- choix d'une technologie adaptée à la taille des données et aux débits nécessaires.

Sur ce point également, certaines solutions fondées sur un recours au « cloud » peuvent se révéler pertinentes et sources d'économies financières.

4. LES RECOMMANDATIONS

Pour en savoir plus, visiter le site de référence de l'ANSSI : http://www.ssi.gouv.fr/ et notamment le MOOC.

En cas de doute ou de manque de compétences, contacter le CERT France (Computer Emergency Response Team) -http://www.cert.ssi.gouv.fr/cert-fr/certfr.html - téléphone national 01 71 75 84 68.

4.1 Pour prévenir le risque cyber

Sur Internet, nul n'est à l'abri d'une action malveillante ou de messages non sollicités. En conséquence, il est utile de suivre les recommandations mentionnées ci-après :

4.1.1 Installer des outils de protection de qualité sur les postes de travail et les réseaux

De nombreux outils de sécurité existent sur le marché, mais au préalable il faut activer et mettre à jour toutes les protections livrées avec le système d'exploitation choisi (anti-virus, pare-feu…). L'acquisition de bons logiciels de protection des postes de travail et des réseaux, avec des mises à jour automatiques, est une première assurance contre les cyber-attaques. Éviter les logiciels gratuits sur internet et l'utilisation de clés USB non désinfectées. L'ANSSI recommande de recourir à des produits bénéficiant de son visa sécurité[11].

Note : une désactivation des ports USB est une sage précaution pour éviter toute intrusion. Les ordinateurs séparés du réseau dénommés « stations blanches » constituent une solution reconnue par l'ANSSI pour limiter les risques liés aux clés USB[12].

4.1.2 Utiliser des mots de passe robustes et les changer régulièrement (postes de travail et fichiers)

Utiliser des mots de passe robustes, permettant d'accéder aux ordinateurs et aux données, fichiers, etc. Il est essentiel de savoir choisir des mots de passe, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne. Voici quelques règles simples :

- choisir des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux). Ou mieux, faire des phrases ;
- utiliser des mots de passe différents pour chaque service, chaque utilisation : messagerie professionnelle, personnelle, documents, accès réseaux… ;
- renouveler les mots de passe avec une fréquence raisonnable et toujours après une mise en service ;

[11] https://www.ssi.gouv.fr/administration/visa-de-securite/
[12] https://www.ssi.gouv.fr/guide/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies/

- configurer les logiciels, le navigateur web, pour qu'ils ne se « souviennent » pas des mots de passe ;

- stocker les mots de passe dans un logiciel sécurisé séparé, pas sur du papier ou un carnet d'adresses.

  Mais soyez conscients qu'il n'existe pas de solutions totalement satisfaisantes.

4.1.3 Supprimer les logiciels ou versions obsolètes et avoir toutes les licences logicielles à jour

Avoir un système d'exploitation et des logiciels mis à jour : navigateur, antivirus, bureautique, pare-feu, etc. La plupart des attaques tentent d'utiliser les failles d'un ordinateur. Les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et parvenir à s'y introduire. Il est donc fondamental de mettre à jour tous ses logiciels afin de corriger ces failles. Une bonne mesure est de ne mettre sur les postes de travail que le strict nécessaire en termes d'applications et de droits d'utilisation, quitte ensuite à implanter de nouveaux logiciels en fonction des besoins opérationnels.

4.1.4 Supprimer l'activation automatique de tous les logiciels rarement utilisés ou inutiles

Désactiver par défaut les composants qui s'installent automatiquement lors de la mise en route d'un ordinateur, qui le ralentissent et qui ne servent souvent à rien. Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle d'une machine vulnérable. Ne les activer que si nécessaire.

4.1.5 Sauvegarder au préalable les données

Il est important de procéder, avant toute tentative de restauration, à une **copie totale du disque**, y compris des secteurs non occupés, car une simple sauvegarde de fichiers ne fournit pas l'intégralité des informations contenues sur le disque. Sans cette copie, les interventions de restaurations altéreraient l'analyse des données et rendraient inefficace toute procédure judiciaire éventuelle ultérieure.

4.1.6 Effectuer des sauvegardes régulières des données et les stocker physiquement sur un site séparé

Effectuer des sauvegardes régulières. Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou à un dysfonctionnement. La sauvegarde de ses données est une condition de la continuité de votre activité. Automatiser et sécuriser les sauvegardes en utilisant des disques doublés interconnectés sur deux sites différents via internet, afin de contrer un vol ou une destruction physique sur l'un des deux sites. Des solutions de mise en œuvre simple au prix d'un bon PC existent. Se méfier des « clouds » pour le stockage des données qui sont souvent des « aspirateurs » d'informations sensibles. Selon les recommandations de l'ANSSI, il est important de mentionner que les données sauvegardées doivent surtout être si possible hors ligne - les « rançongiciels » actuels commençant par chiffrer les sauvegardes, qu'elles soient sur un site distant ou non.

4.1.7 Navigation sur internet

Paramétrer le navigateur internet afin de supprimer automatiquement toute trace de navigation, notamment les cookies et les historiques de navigation afin de ne pas laisser de trace de ses habitudes sur l'ordinateur, ces traces étant utilisées par les sites contactés pour des actions de télémarketing voire d'intrusion. Ne jamais autoriser le navigateur à mémoriser les mots de passe, car ce sont souvent les mêmes qui sont utilisés pour des applications internes, permettant l'accès aux autres données plus sensibles. Ces règles d'hygiène informatique ont pour contrepartie de devoir réintroduire toutes les données lors d'une connexion mais c'est le prix de la tranquillité. Bien entendu pour toute transaction sensible sur internet n'utiliser que les sites sécurisés en "https" précédés d'un petit cadenas.

4.1.8 Séparer les comptes administrateurs et les comptes utilisateurs

L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci qui permettent ou non de conduire certaines actions et d'accéder à certains fichiers de l'ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits d'utilisateur. Le compte administrateur ne doit être utilisé que par l'administrateur.

Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour exploiter des logiciels, envoyer des messages ou surfer sur l'Internet. En limitant les droits d'un utilisateur, on limite aussi les risques d'infection ou de compromission de l'ordinateur. Il convient de réduire a minima le nombre de titulaires de comptes disposant de privilèges.

4.1.9 Filtrer et identifier les messages extérieurs par rapport aux messages internes

Identifier formellement les échanges de messages internes, par les noms de domaines ou adresses, de ceux provenant de l'extérieur, en paramétrant le logiciel de messagerie. Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement, fait parvenir un message surprenant, il convient de ne pas l'ouvrir et surtout pas les pièces jointes ou les liens inclus dans le message. En cas de doute, il est toujours possible de valider l'échange par téléphone sinon détruire définitivement ce type de message. Il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et répondre sans un minimum de précaution. À l'inverse, quand on envoie des fichiers en pièces jointes, privilégier les formats les plus « inertes » possible, comme RTF ou PDF, cela limite les risques de fuites d'informations.

Disposer de mails différents selon les usages (pro, perso, confidentiel, achats en ligne, etc.) ;

Dans toute la mesure du possible, séparer numériquement vie professionnelle et vie privée.

4.1.10 S'appuyer sur des spécialistes (internes ou externes)

Aujourd'hui, le niveau de risque est tel que seuls des spécialistes sont à même de traiter ces questions. L'entreprise peut alors faire appel à de la sous-traitance ou, si elle en a les moyens et que les enjeux le justifient, créer un poste de responsable en charge de la sécurité des systèmes d'informations (RSSI).

Nota : La personne en charge de la fonction RSSI doit être clairement identifiée par tous les administrateurs système/réseau ou par les utilisateurs en particulier dans les PME/PMI.

4.1.11 Créer un réseau privé virtuel sécurisé (VPN)

S'il y a plusieurs postes de travail interconnectés, établir un VPN (Réseau WIFI ou filaire protégé avec mot de passe…) pour interconnecter les postes sur un seul routeur (a minima une Box). Ce routeur, lui aussi sécurisé, doit être le seul point d'accès externe à l'internet

(une seule porte d'entrée et de sortie sur le monde connecté est plus sûre et l'existence d'une fenêtre via l'utilisation d'un « smartphone » ou autre avec la 4G est proscrite …) ;

Éviter de connecter sur le VPN, une machine nomade ou venant de l'extérieur dont on ne connaît pas l'origine. Dans le même esprit, éviter l'installation externe de « Démos », clés USB, Smartphone… ;

Nota : il est recommandé d'éteindre électriquement les équipements connectés (PC, Machines…) quand ils ne sont pas utilisés (le soir et le week-end…). Outre des économies d'énergies notables, la sécurité sera renforcée et les mises à jour se feront automatiquement à la remise en route.

4.2 Pour se protéger en cas de cyber attaque

Avant tout il sera nécessaire d'effectuer régulièrement un suivi des recommandations (pour éviter la routine) et des audits internes de sécurité. Ensuite mener à froid avec un expert un exercice de cyber attaque afin de tester les mesures mentionnées ci-dessous. Si le processus ci-après semble trop complexe, il faut au moins isoler les postes de travail du réseau et ensuite faire appel à des spécialistes ou au CERT cité en début des recommandations.

4.2.1 Informer la personne en charge de la fonction (RSSI)

Prévenir immédiatement le sous-traitant ou le RSSI interne qu'une intrusion a été détectée. C'est la base de toute procédure de réaction sur incident de sécurité

4.2.2 Rechercher les traces de compromission

Un équipement n'est jamais isolé dans un système d'information. S'il a été compromis, il doit exister des traces dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.). C'est pourquoi il est utile de rechercher des traces liées à la compromission dans tout l'environnement, les copier, les dater et les signer numériquement. Cette recherche est effectuée par la personne en charge de la fonction RSSI qui se fait aider en tant que de besoin par des spécialistes ou par le CERT.

4.2.3 Déconnecter les machines compromises

Déconnecter immédiatement du réseau la (les) machine(s) compromise(s) permet de stopper l'attaque si elle est toujours en cours. Ainsi l'intrus n'a plus de contrôle sur le (les) équipement(s) connecté(s) et ne pourra donc pas poursuivre son intrusion malveillante. Maintenir la machine sous tension et ne pas la redémarrer, car il serait alors impossible de connaître les processus qui étaient actifs au moment de l'intrusion. Et cela risquerait de provoquer une modification sur le système de fichiers et de perdre de l'information utile pour l'analyse de l'attaque.

4.2.4 Éviter de se connecter avec l'agresseur

Si l'origine probable de l'intrusion est déterminée, ne pas essayer d'entrer en contact directement avec l'agresseur, surtout en cas de demande de paiement de rançon. Ceci risquerait d'entraîner une connexion avec le pirate et de lui fournir des informations sur votre démarche et votre connaissance de sa présence.

4.2.5 Analyser l'incident avec prudence

L’analyse interne de l’incident ne devra être faite que sur une deuxième copie physique du disque dur. L’altération des données provoquée par l’analyse de la première sauvegarde rendrait inefficace toute procédure judiciaire.

Les grandes étapes de l’analyse de l’intrusion sont :

a. Recherche des modifications dans le système et les fichiers de configuration ;

b. Recherche des modifications de données ;

c. Recherche des outils et des données laissés par l’intrus ;

d. Examen des fichiers de journalisation ;

e. Vérification des autres machines connectées sur le réseau.

4.2.6 Réinstaller le système d’exploitation

Réinstaller complètement le système d’exploitation à partir d’une version saine. Ne pas oublier que sur une machine compromise, n’importe quelle partie du système d’information peut avoir été modifiée : noyau, binaires, fichiers de données, processus et mémoire. D’une manière générale, la seule manière de s’assurer qu’une machine ne possède plus de porte dérobée ou autre modification laissée par l’intrus, est de réinstaller entièrement le système d’exploitation à partir d’une distribution saine et de compléter cette installation en appliquant tous les correctifs de sécurité, avant de reconnecter la machine à un réseau.

4.2.7 Réinstaller en priorité les applicatifs de sécurité

Pour finir, réinstaller en priorité les applicatifs de sécurité avant de se reconnecter sur le réseau, puis les applicatifs mis à jour en leur appliquant les correctifs de sécurités recommandés, supprimer tous les services inutiles, changer tous les mots de passe, refaire une analyse de sécurité du poste de travail et enfin, restaurer les données.

4.2.8 Entrer en relation avecl’ANSSI

En appliquant les recommandations mentionnées sur le site https://www.ssi.gouv.fr/en-cas-dincident/.

5 CONCLUSION

Nous avons traité, dans nos précédents cahiers, des plans de continuité d'activité (cahier n° 24) et des facteurs humains et organisationnels dans la gestion des risques (cahier n° 28). Nous ne pouvons qu'inviter le lecteur à les consulter car ces cahiers ont aussi pour objectif d'aider les PME/PMI, en posant des questions pragmatiques sur ces sujets d'actualité.

Nous avons adopté la même démarche pour aborder le risque de cyber-sécurité, ce qui explique que certaines recommandations sont du même type, car ce sont tout autant d'outils qui forgent la résilience de l'entreprise.

Force est de constater que la transformation digitale est utilisée principalement comme source d'opportunités. Mais, toutes les organisations et la quasi-totalité des entreprises sont dépendantes du numérique et se trouvent donc, directement ou non, exposées à des cyber-attaques. D'ailleurs, les PME étant des cibles particulières doivent être vigilantes sur leurs vulnérabilités, car les conséquences peuvent être dramatiques pour leur pérennité.

Face au sentiment - assez fréquent parmi certaines PME - que lutter contre les cyber-attaques est une démarche trop coûteuse et qui plus est, nécessite un bagage trop technique, ce cahier s'est fixé comme objectif d'apporter des solutions simples et claires en proposant les parades nécessaires et indispensables à des infiltrations dans les systèmes d'informations par des personnes mal intentionnées.

Grâce aux multiples propositions présentées dans ce cahier, les PME-PMI pourront disposer d'une vision globale des précautions à prendre par l'entreprise, non seulement sur le plan technique mais aussi sur les plans humain et organisationnel, car les entreprises sont vulnérables sur l'ensemble de ces plans.

Et pour terminer ce cahier par une touche optimiste, on peut constater que la mutation numérique et la cyber-sécurité donnent des occasions de création d'entreprises, de développement des activités de services et de conseils et d'amélioration de la résilience.

6 LES TÉMOIGNAGES

Sources de presse

- Article Altran : Source : https://www.zdnet.fr/actualites/ransomware-dominique-cerutti-pdg-d-altran-mon-1er-conseil-assurez-vous-39895949.htm.:
- Cadiou-Industrie : Source : Le Télégramme.

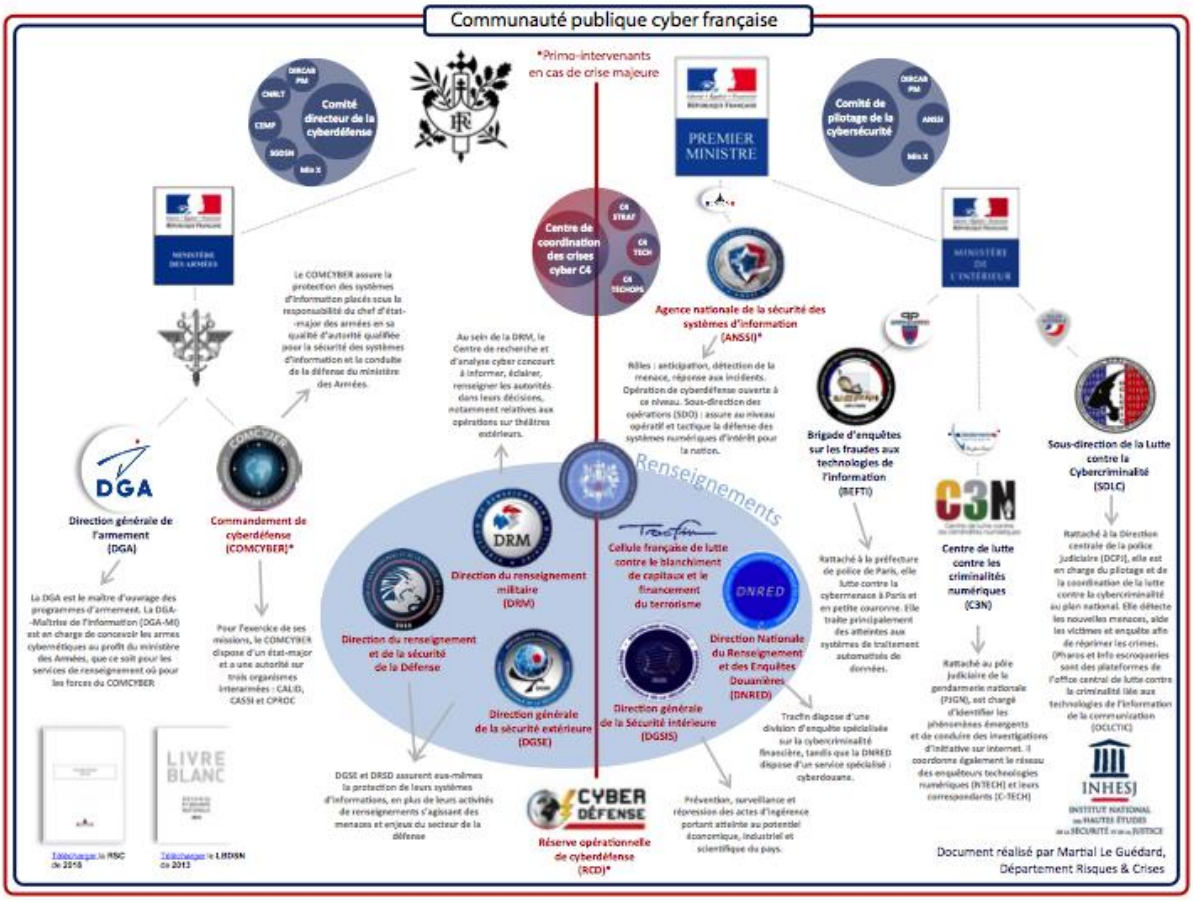
7 RÉFÉRENCES, BIBLIOGRAPHIE& SITES UTILES

7.1. Concernant la cyber sécurité

- 2013_02_26 The Real Story of Stuxnet https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet
- 30 déc. 2014 Nuclear Power Plant Cybersecurity https://www.linkedin.com/pulse/nuclear-power-plant-cybersecurity-george-moraetes?goback=%2Egde_46854_member_5964795954149228546
- 2015, année noire pour la cybersécuritéhttp://www.usine-digitale.fr/article/2015-annee-noire-pour-la-cybersecurite.N370382
- CYBER RESILIENCE Cyber security and business resilience it Governance Report January 2015
- Le site du ministère de la Défense paralysé ce mardi 6 janvier 2015, 7 janvier 2015, http://www.zone-numerique.com/anonymous-le-site-du-ministere-de-la-defense-paralyse-ce-mardi-6-janvier-2015.html
- L'hébergeur OVH visé par la plus violente attaque DDoS jamais enregistrée (1Tbps), 25 septembre 2016 https://www.undernews.fr/hacking-hacktivisme/lhebergeur-ovh-vise-par-la-plus-violente-attaque-ddos-jamais-enregistree-1tbps.html
- Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Approvisionnement en énergie électrique » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense NOR: PRMD1621026A
  ELI: https://www.legifrance.gouv.fr/eli/arrete/2016/8/11/PRMD1621026A/jo/texte
- Arrêté du 11 août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives au sous-secteur d'activités d'importance vitale « Transports maritime et fluvial » et pris en application des articles R. 1332-41-1, R. 1332-41-2 et R. 1332-41-10 du code de la défense NOR: PRMD1620550A
  ELI: https://www.legifrance.gouv.fr/eli/arrete/2016/8/11/PRMD1620550A/jo/texte
- Cyberattaques, pénurie d'eau et changement climatique, les trois Némésis de l'énergie mondiale 20/09/2016 http://www.usinenouvelle.com/article/cyberattaques-penurie-d-eau-et-changement-climatique-les-trois-nemesis-de-l-energie-mondiale.N439767
- Mutually assured cyber destruction? DAVID HOROVITZ 15 December 2016 https://www.timesofisrael.com/mutually-assured-cyber-destruction/
- Timely implementation of security in power plant industrial control systems at the construction stage is vital, 2017_01_11 http://www.powerengineeringint.com/articles/print/volume-25/issue-10/features/the-anatomy-of-ics-cybersecurity.html
- Inde: le port de Bombay affecté par la cyber-attaque mondiale, AFP28/06/2017, http://www.lepoint.fr/monde/inde-le-port-de-bombay-affecte-par-la-cyberattaque-mondiale-28-06-2017-2138904_24.php
- Hackers are targeting Nuclear Facilities, Homeland Security Dept. and FBI say https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html
- Cyber-attaques : qui est l'ennemi ? Claire Gerardin | 20/07/2017, http://www.latribune.fr/opinions/tribunes/cyberattaques-qui-est-l-ennemi-744537.html
- Les ransomwares ont extorqués 25 millions de dollars à travers le monde 27/07/2017 http://www.01net.com/actualites/les-ransomwares-ont-extorques-25-millions-de-dollars-a-

travers-le-monde-1224952.html#utm_term=Autofeed&utm_campaign=Echobox&utm_medium=Social&utm_source=Twitter&link_time=1501151272
- LA PROTECTION DES DONNÉES PERSONNELLES CSA Research Septembre 2017 / Étude n°1700780
- Le réseau électrique français peut-il être piraté ? LE MONDE | 08.12.2017 http://www.lemonde.fr/pixels/article/2017/12/08/le-reseau-electrique-francais-peut-il-etre-pirate_5226462_4408996.html
- The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies Jordan Robertson and Michael Riley 4 octobre 2018 https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
- Meltdown/Spectre : ce qu'il faut savoir sur la faille des processeurs Intel, Apple et Microsoft dans la tourmente, 04/01/18 https://www.lesnumeriques.com/informatique/meltdown-spectre-qu-faut-savoir-sur-faille-processeurs-n69881.html
- Cybersecurity: How utilities can prepare the next generation smart grid, 02/12/2018 Scott Foster, Chief Executive of Delta Energy & Communications http://www.powerengineeringint.com/articles/2018/02/cybersecurity-how-utilities-can-prepare-the-next-generation-smart-grid.html?cmpid=enl_pei_peidigest_2018-02-12&pwhid=fd0a0c199dd663a003472072ef331b2e7ba42025f9a7e6230fd655c5655455aa05636f7d35b5fd26d41fedf0c08e227bc6be9862319240306944b831e29e49f6&eid=296409644&bid=2001019
- A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
- The NIS Directive will mitigate the sixth biggest threat facing humanity Luke Irwin 9th April 2018 https://www.itgovernance.eu/blog/en/the-nis-directive-will-mitigate-the-sixth-biggest-threat-facing-humanity?utm_source=Email&utm_medium=Macro&utm_campaign=S01&utm_content=2018-06-05
- ÉTAT DE LA MENACE LIÉE AU NUMÉRIQUE EN 2018 LA RÉPONSE DU MINISTÈRE DE L'INTÉRIEUR Rapport n° 2 Mai 2018 Délégation ministérielle aux industries de sécurité et à la lutte contre les cyber-menaces
- Comment se protéger des cyber-malveillances ? Le gouvernement propose un kit de conseils, Marius François14/06/2018 http://www.lefigaro.fr/secteur/high-tech/2018/06/14/32001-20180614ARTFIG00302-comment-se-proteger-des-cybermalveillances-le-gouvernement-propose-un-kit-de-conseils.php
- Estimer le cyber-risque pour le secteur financier Christine Lagarde 22 juin 2018 https://www.imf.org/external/french/np/blog/2018/062218f.htm
- TRITON : retour sur une attaque des systèmes de contrôle industriel qui a sérieusement perturbé l'exploitation d'une infrastructure critique décembre 14, 2017 https://www.fireeye.com/blog/fr-threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html
- Appel de Pris pour la confiance et la sécurité dans le cyberespace, 2018_11_12
- Baromètre des risques Allianz 2019 : la France inquiète sur la cybersécuritéhttps://www.faceaurisque.com/2019/01/15/barometre-des-risques-allianz-2019-la-france-inquiete-sur-la-cybersecurite/
- La France se dote d'une doctrine militaire offensive dans le cyberespace et renforce sa politique de lutte informatique défensive18/01/2019, **Éléments publics de doctrine militaire de lutte informatique OFFENSIVE** (format pdf, 398.36 KB), **Politique ministérielle de lutte informatique DEFENSIVE** (format pdf, 417.72 KB).
- Après les fake news, la menace du «deepfake» prend de l'ampleur sur le web**,** Harold Grand, 02/01/2019 http://www.lefigaro.fr/secteur/high-tech/2019/01/02/32001-

20190102ARTFIG00162-apres-les-fake-news-la-menace-du-deep-fake-prend-de-l-ampleur-sur-le-web.php
- Du cyber et de la guerre, O. Kempf, Fondation pour la Recherche Stratégique, Note n°17/19, 12 septembre 2019
- A Practical Guide to Building an Effective Cybersecurity Strategy for Your Power Grid, Guide Indegy, August 2019
- Le cyber Campus Britannique: un projet majeur d'investissement post COVID 19 de 2 milliards de livres. Bernard Barbier, May 28, 2020, https://www.linkedin.com/pulse/le-cyber-campus-britannique-un-projet-majeur-post-covid-barbier/?trackingId=NuCM6hytSxKGp0osn1oU9A%3D%3D&fbclid=IwAR0TMsnFKwXLaSrLMKc2Tby-X0DFe3DQGMPeY631ug6TTbLKuYJIow6nkHY
- GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE 12 règles essentielles pour sécuriser vos équipements numériques, CPME-ANSSI Version 1.1.1 - Septembre 2017.
- La cyber-sécurité dans le monde portuaire, D. Kechemair et J. Besancenot, Magazine IESF n°3, 1er trimestre 2019, dossier Numérique et Cyber-sécurité.
- Preparing cyber insurance – FERMA, 2019
- Maitrise du risque numérique AMRAE-ANSSI, 2020.
- Les acteurs de la communauté publique cyber-française



7.2 Bibliographie et sites utiles

[1]https://www.pole-excellence-cyber.org/wp-content/uploads/2019/11/Référentiel-Cyber-V5.0.pdf
[2]https://www.defense.gouv.fr/content/download/551555/9394645/Eléments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf
[3]https://www.lemondeinformatique.fr/actualites/lire-panocrim-2019-le-clusif-livre-son-etat-des-lieux-de-la-cybercriminalite-77814.html
[4]https://www.ssi.gouv.fr/actualite/rancongiciels-lanssi-livre-son-analyse-de-la-menace-pour-les-entreprises-et-les-institutions/
[5] Source Guide 2019-2020 cyber-sécurité Hors-série Solutions Numériques
[6] https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/
[7] https://www.ssi.gouv.fr/administration/visa-de-securite/
[8] Source : « Sécurité Opérationnelle, Conseils pratiques pour sécuriser le SI », Alexandre Fernandez-Toro, Eyrolles
[9]https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail
[10] https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-
[11] https://www.ssi.gouv.fr/administration/visa-de-securite/
[12] https://www.ssi.gouv.fr/guide/profil-de-fonctionnalites-et-de-securite-sas-et-station-blanche-reseaux-non-classifies/
[13] https://oxi90.com/ZXIICTS33/AA77257181C34F0F9500D4FA6958CCFA.php

7.3 Nos cahiers

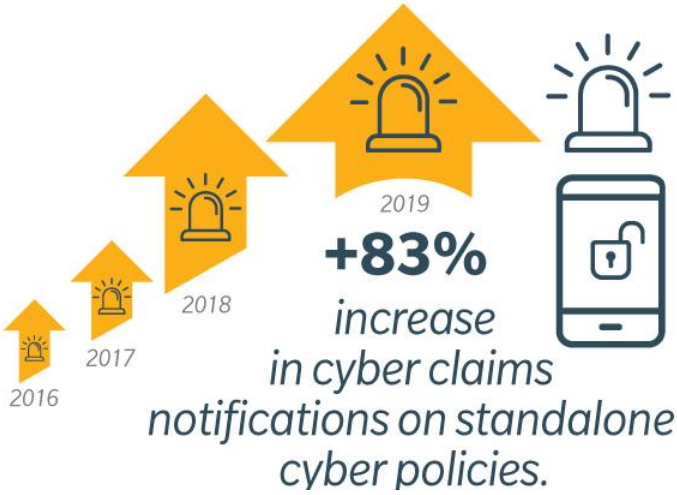
Ces cahiers sont téléchargeables gratuitement sur : www.iesf.fr

- **IESF Cahier n° 2 –** Contributions de l'Ingénieur à la maîtrise des risques.
- **IESF Cahier n° 4 -** Conseils aux dirigeants de PME-PMI - Comment protéger votre entreprise des fraudes, négligences ou malveillances.
- **IESF Cahier n° 17 –** Dirigeants de PME-PMI - Comment évaluer la vulnérabilité de votre activité par un autodiagnostic - Des pistes pour mieux maîtriser vos risques.
- **IESF Cahier n° 24 –** Plan de Continuité d'Activité
- **IESF Cahier n° 28 –** Influence des facteurs humains et organisationnels sur la maîtrise des risques

8. ANNEXES

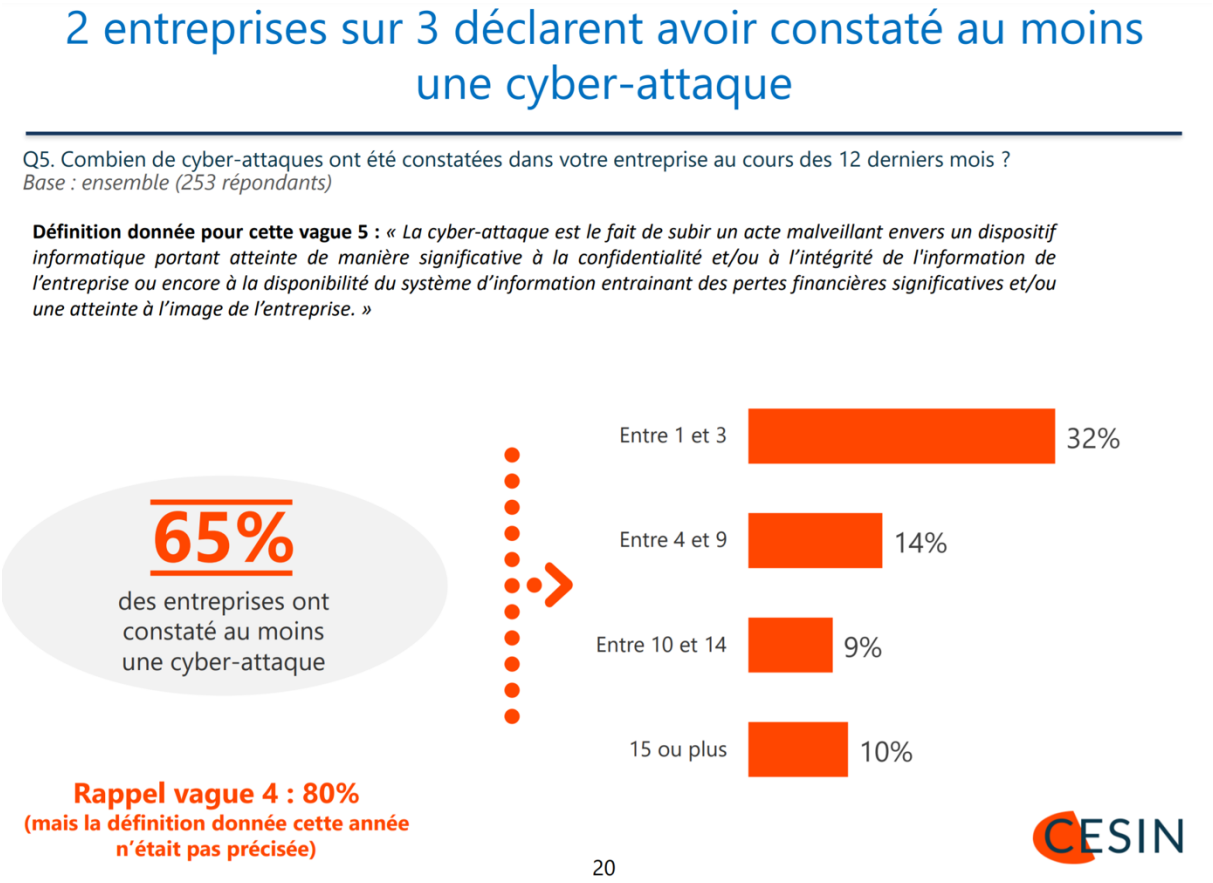
Annexe 1 – Constats et statistiques

1.1 Augmentation annuelle du nombre de cyber-attaques en Europe

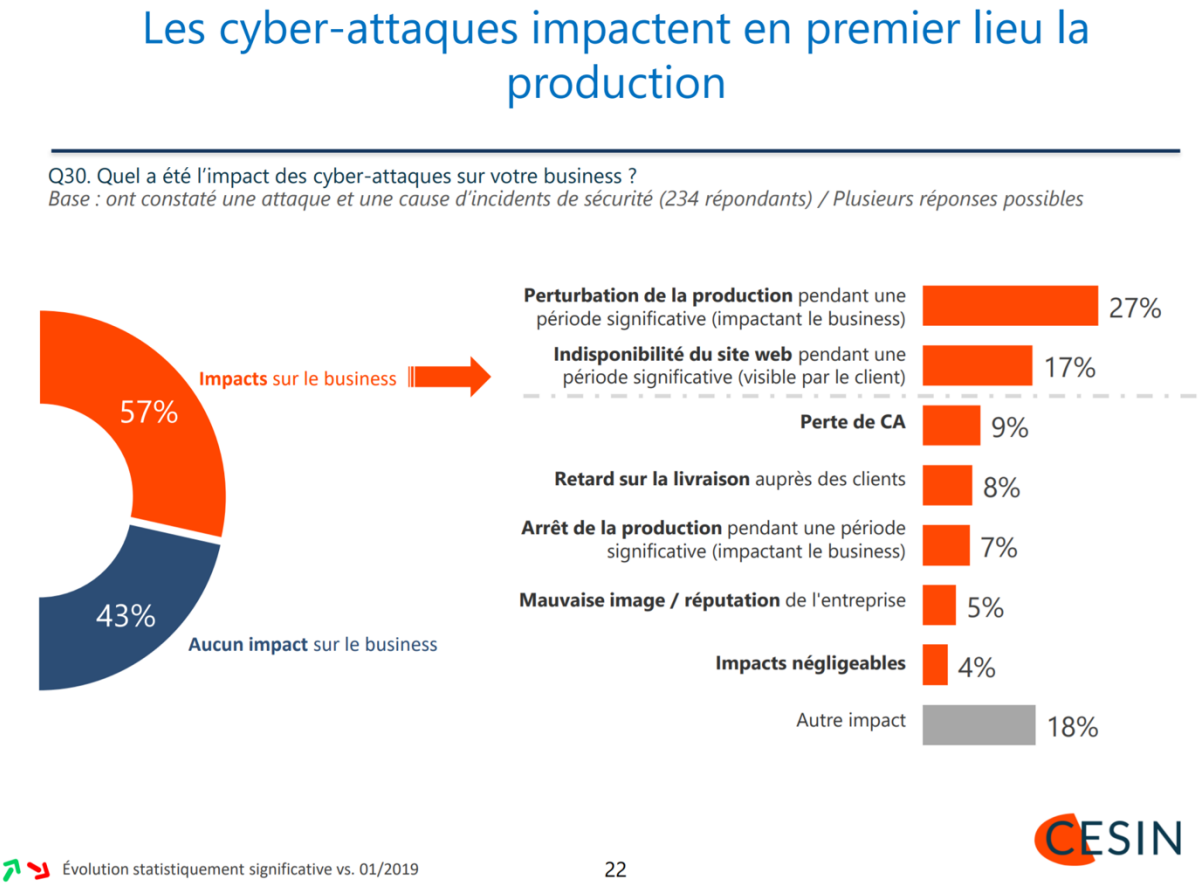


Source Marsh

1.2 Enquête auprès des entreprises



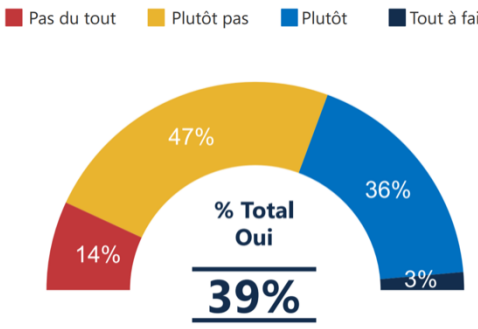
1.3 Impact des cyber-attaques sur les entreprises



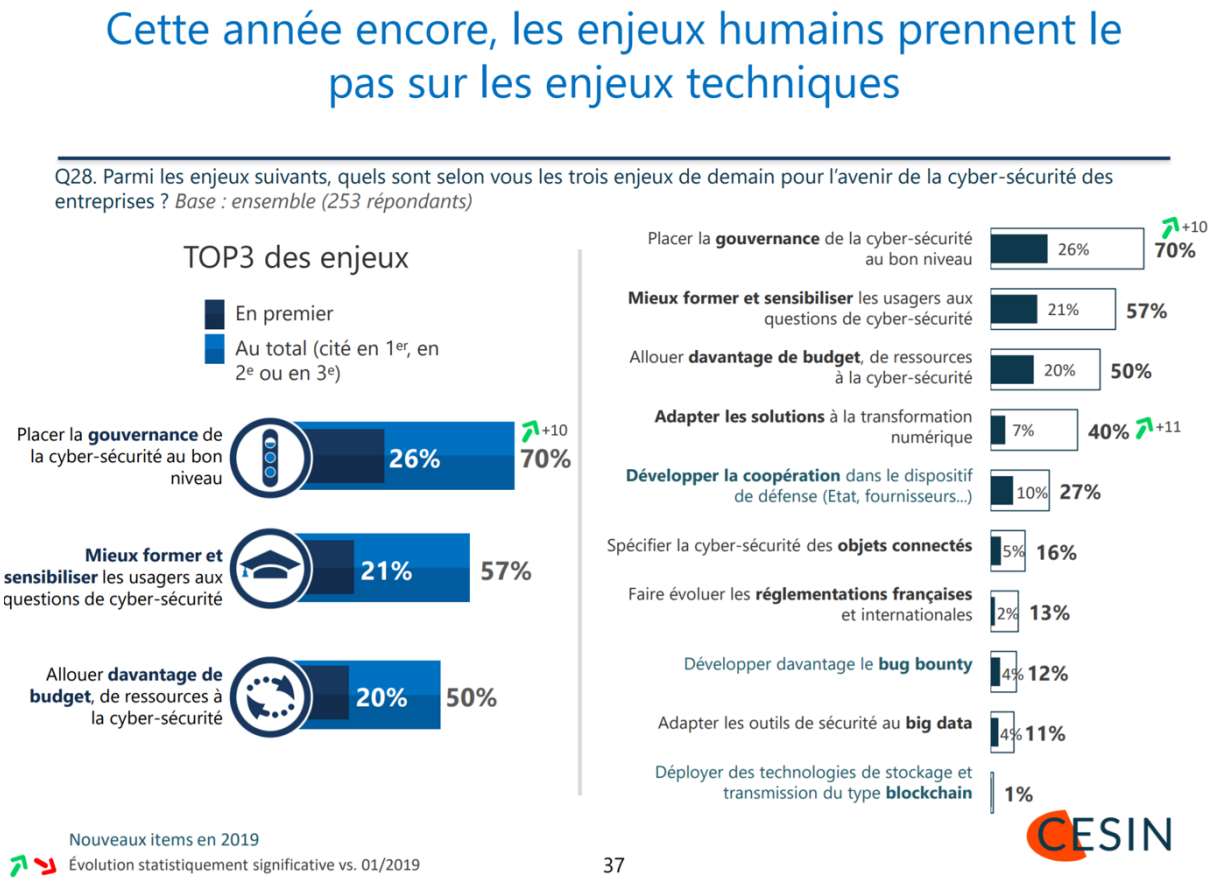
1.4 Préparation des entreprises face aux cyber-attaques

Seules 4 entreprises sur 10 se disent préparées en cas de cyber-attaque de grande ampleur

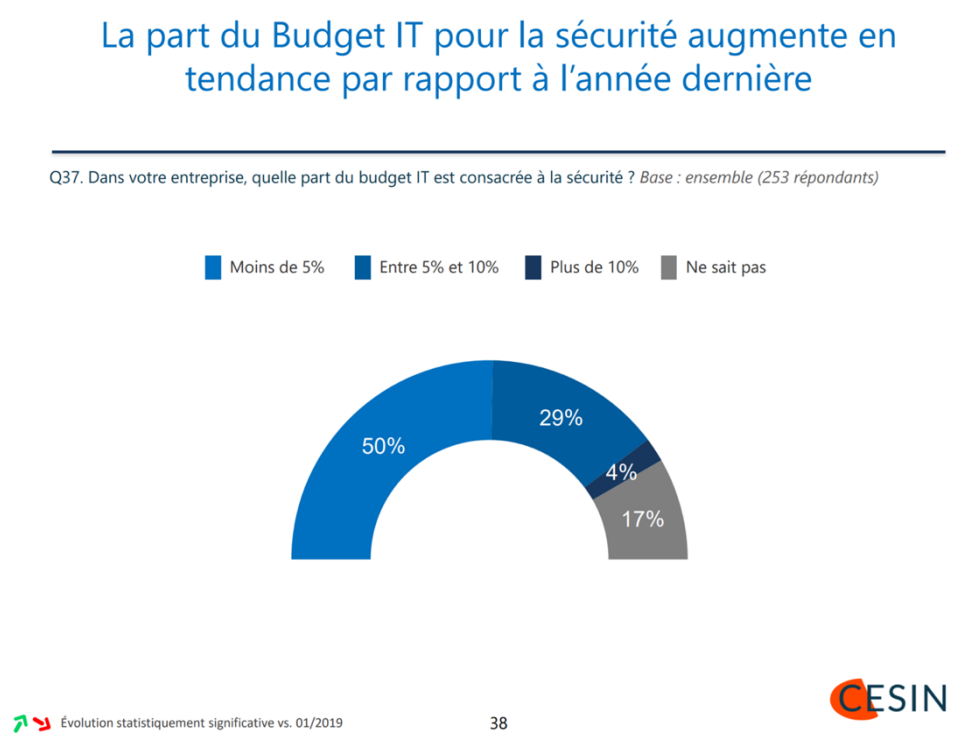
Q38. Selon vous, votre entreprise est-elle préparée à gérer une cyber-attaque de grande ampleur ?
Base : ensemble (253)



1.5 Appréciation des entreprises sur trois enjeux de demain pour leur cyber-sécurité.



1.6Part du budget



Annexe 2 – Lexique

APT

Une APT (Advanced Persistent Threat), ou menace persistante avancée, est un piratage informatique qui vise à placer du code malveillant personnalisé sur des postes de travail. Et ceci en restant inaperçu le plus longtemps possible.

Botnet

Réseau d'équipements compromis (ordinateurs, serveurs, périphériques, etc.) par des logiciels malveillants et piloté à distance par un ou des cyber-attaquants pour envoyer par exemple des courriers électroniques non désirés, lancer des attaques par déni de service, se procurer des droits privilégiés, voler ou altérer des informations... Certains de ces réseaux peuvent atteindre plusieurs milliers de machines

Cryptolocker

Un « cryptolocker » ou crypto-verrouilleur est un « ransomware » diffusé principalement par des courriels infectés, qui crypte les données de l'utilisateur. Une rançon est demandée (souvent en bitcoins) pour obtenir les clefs de chiffrement.

Malware

Un « malware » (malicious software ou logiciel malveillant) est un programme informatique développé dans le but de nuire. Virus, vers, cheval de Troie sont des malwares très répandus.

Transformation digitale

La transformation digitale désigne le processus qui consiste, pour un organisme, à intégrer pleinement les technologies digitales dans l'ensemble de ses activités.

Digitalisation

Digital : Synonyme et terme anglais pour « numérique », il regroupe communément un ensemble de technologies/usages comme les nouvelles technologies liées à la virtualisation (Dockers…), tout ce qui concerne la donnée (prédictif, « big data »…), la mobilité, les méthodes agiles, le « Time to Market ».

Numérisation

Évolution des sens Numérique / Digital : La « numérisation » vise aujourd'hui la dématérialisation des données et la gestion des outils qui permettent de les traiter. La « digitalisation » vise plus les modes de travail, d'organisation, de management, de gestion du capital humain et de stratégie ouverts par les possibilités technologiques et l'évolution des mentalités.

Intelligence artificielle

L'expression « intelligence artificielle » fut proposée en 1955 par l'un des initiateurs du Summer Camp de Darmouth, John McCarthy. Elle recouvre les sciences et technologies qui permettent d'imiter, d'étendre et/ou d'augmenter l'intelligence humaine avec des machines. Une autre définition courante définit l'IA comme le champ académique de création de logiciels et matériels doté de certaines formes d'intelligence.

GDPR

Règlement général sur la protection des données **General Data Protection Regulation.**

IOT

Internet of Things ou Internet des objets

Phishing ou Hameçonnage

Consiste à usurper une identité afin d'obtenir des renseignements personnels ou de identifiants bancaires pour en faire un usage criminel. Les escrocs se font passer pour un tiers de confiance.

Spearphishing

(Littéralement pêche au harpon) est un mélange de techniques classiques de hameçonnage et d'ingénierie sociale. Ce volet ingénierie sociale permet de cibler l'attaque en utilisant des thèmes liés au travail quotidien ou aux intérêts de la cible.

Ransomware

Un « ransomware » ou « rançongiciel » est un programme informatique qui bloque l'accès aux données tant qu'une rançon n'a pas été payée.

DDOS (Distributed Denial of Service)

Une attaque par déni de service consiste à rendre indisponible un serveur, principalement en le saturant par un trop grand nombre de requêtes simultanées.

SOC (Security Operations Center)

Un SOC, dans une entreprise, désigne une division qui assure la sécurité de l'organisation et surtout le volet sécurité de l'information.

Signature digitale

Méthode informatique qui permet de transmettre une signature par un certificat vérifié par chiffrement asymétrique pour garantir l'identité de l'émetteur.

Annexe 3 - Quelques recommandations particulières

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) assure la mission d'autorité nationale et elle apporte en particulier son expertise et son assistance technique aux administrations et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV) et des Opérateurs de Service Essentiel (OSE).À ce titre, l'ANSSI diffuse de nombreux documents de sensibilisation et de recommandations à l'intention de différents publics, comme par exemple un guide et de nombreux supports sur la méthode EbiosRisk Manager, qui constitue la méthode de référence d'analyse de risques dans le domaine de la Sécurité des Systèmes d'Information.

Les services de l'État (ANSSI, DGSI) organisent régulièrement des réunions de sensibilisation avec interventions de « témoins » dans un but de sensibilisation.

La gendarmerie nationale s'est également organisée pour assurer ses missions face à ces nouvelles menaces et a par exemple consacré son édition de décembre 2019 de sa revue trimestrielle (n°266) au thème de « l'humain au cœur de la cyber-sécurité »

Par ailleurs, un "écosystème" d'entreprises s'organise depuis plusieurs années, permettant de favoriser les échanges de bonnes pratiques :

- CESIN : club des experts de la sécurité de l'information et du numérique ;
- CIGREF : grandes entreprises et administrations utilisatrices de solutions numériques, a produit un « Serious Game » : « Keep an Eye Out », sur la cyber ;
- Cyber-cercle : cercle de réflexion sous la dynamique des élus, parlementaires et locaux ;
- CLUSIF : Club de la sécurité de l'information français, publication MIPS (Menaces Informatiques et Pratiques de Sécurité), actif en normalisation avec AFNOR, a publié un Livre Blanc « La cyber-sécurité à l'usage des Dirigeants » (édition 2020 disponible) ;
- CNIL : données personnelles : régulateur (RGPD) mais aussi enquêtes et sanctions ;
- HEXATRUST : groupement d'entreprises : offres de produits innovants ;
- Syntec Numérique : syndicat professionnel des 2000 entreprises de services du numérique, éditeurs de logiciels et sociétés de conseil, comité cyber-sécurité créé en 2015 ;

Au-delà du retour d'expérience sur des incidents ou des attaques, il est également utile :

- d'observer le retour d'expérience en termes de bénéfices d'entreprises ou d'organisation ayant amélioré leur protection et leur organisation face au risque cyber : démontrer une démarche active en la matière peut être en effet un atout différentiant de compétitivité pour l'entreprise face à la concurrence,
- de parcourir la Lettre INHESJ n°6 - juillet 2020[13]

[13] https://oxi90.com/ZXIICTS33/AA77257181C34F0F9500D4FA6958CCFA.php

Annexe 4 – Fiche d'autodiagnostic

1. Avez-vous une installation industrielle pilotable depuis l'extérieur de votre site ?
2. Avez-vous une installation technique bénéficiant d'une télémaintenance ?
3. Avez-vous des IoT (Internet Of Things - Objets connectés) sur votre informatique ?
4. Avez-vous rencontré des problèmes dus à l'obsolescence de systèmes informatiques (matériel ou logiciel) ?
5. Avez-vous des procédures de mise à jour régulière des logiciels (notamment les anti-virus) ?
6. Avez-vous des procédures pour les accès informatiques et la gestion des mots de passe ?
7. Avez-vous une véritable séparation entre les réseaux intranet et internet ?
8. Le matériel nomade du personnel utilise-t-il des données chiffrées ?
9. Avez-vous des procédures sécurisées pour les transferts de fichiers ?
10. Avez-vous bloqué les ports USB et la connexion Bluetooth de vos ordinateurs ?
11. L'accès à distance à votre réseau se fait-il uniquement par un Réseau Virtuel Privé (VPN) ?
12. Traitez-vous des données privatives de personnes physiques ?
13. Avez-vous un service informatique interne à l'entreprise ?
14. Sous-traitez-vous tout ou partie de votre informatique ?
15. Vos sauvegardes sont-elles testées régulièrement (perte d'intégrité cohérence fonctionnelle) ?
16. Pensez-vous maîtriser les risques d'attaque informatique ?
17. Les salariés sont-ils sensibilisés aux cyber-risques ?
18. Existe-t-il une surveillance des cyber-attaques internes ou externes ?
19. Existe-t-il une procédure de remontée d'alerte ?
20. Avez-vous déjà fait appel à une société spécialisée en cyber-risques ?
21. Avez-vous un Responsable Sécurité Informatique (RSI) interne ?
22. Avez-vous déjà été confronté à une cyber-attaque informatique ?
23. Avez-vous une assurance spécifique pour les Cyber-risques ?
24. Pensez-vous que votre entreprise pourrait restreindre l'usage de l'informatique dans certains secteurs ?
25. Avez-vous envisagé des solutions pour produire malgré une panne informatique de longue durée ?
26. Disposez-vous d'une cellule décisionnelle chargée de la gestion d'une crise en cas d'attaque informatique ?

Références

- **AGREPI** (Association des spécialistes de la maîtrise et du management des risques), www.agrepi.com
- **AMRAE** (Management de Risques et des Assurances de l'Entreprise), www.amrae.fr
- **ANSSI** (Agence nationale de la sécurité des systèmes d'information), www.ssi.gouv.fr
- **Base ARIA** (Analyse, Recherche et Information sur les Accidents), www.aria.developpement-durable.gouv.fr
- **CCA** (Club de la Continuité d'Activité, association de praticiens de la continuité d'activité), www.clubpca.eu
- **CNPP,** www.cnpp.com
- **CRIP** (Club des Responsables d'Infrastructures et de Production), www.crip-asso.fr
- **FERMA** (Federation of European Risk Management Associations), www.ferma.eu
- **FFA** (Fédération Française de l'Assurance), www.ffa-assurance.fr
- **ICSI** (Institut de Culture de Sécurité Industrielle), www.icsi-eu.org
- **INERIS** (Institut National de l'Environnement industriel et des RISques), www.ineris.fr
- **INRS** (Institut National de Recherche et de Sécurité pour la prévention des accidents du travail et des maladies professionnelles), www.inrs.fr
- **INSEE** (Institut National de la Statistique et des Etudes Economiques), www.insee.fr
- **IMdR** (Institut pour la Maîtrise des Risques), www.imdr.fr
- **SGDSN** (Secrétariat Général de la Défense et de la Sécurité Nationale), www.sgdsn.gouv.fr