GESTE

LIVRE BLANC

CYBERSECURITÉ ET MÉDIAS

À DESTINATION DES DIRIGEANTS ET ACTIONNAIRES

SOMMAIRE

ÉDITORIAL

Chers membres,

Force est de constater que les médias, dans toute leur diversité, sont de plus en plus ciblés par des cyberattaques, mettant ainsi en péril la liberté de l'information et la pluralité des opinions. Avec l'essor des technologies avancées et la digitalisation constante de nos activités, ces menaces sont devenues omniprésentes. Ces risques ne peuvent et ne doivent plus être sous-estimés. La cybersécurité doit, au contraire, être érigée en priorité stratégique de nos organisations.

> La résilience de nos médias dépend de notre capacité à anticiper et à contrer ces attaques avec détermination et efficacité.
> Dirigeants et décideurs doivent en être parfaitement conscients.

Depuis septembre 2023, le GESTE travaille ainsi à l'élaboration d'un Livre Blanc très opérationnel. Co-écrit par vos pairs et par des experts engagés auprès des éditeurs, il a pour objectif de vous fournir les outils essentiels vous permettant d'appréhender et de répondre efficacement à ces enjeux. Soyons tous proactifs et engagés pour préserver nos valeurs et garantir un avenir sécurisé pour nos médias !

Bertrand GIÉ
Président du GESTE

LES 14 COMMANDEMENTS

AVANT L'ATTAQUE

01 Cartographier ses actifs et évaluer les risques et leurs impacts

02 Allouer des moyens à la sécurité, par la mise en place de mesures adaptées (interne et sous-traitants)

03 Adopter un dispositif de gestion de crise en nommant un comité de gestion de crise

04 Former les équipes et les dirigeants

05 Se faire auditer et s'entraîner en simulant une crise pour tester la task force de crise

DURANT L'ATTAQUE

06 Mesurer l'impact de l'attaque et isoler les actifs concernés

07 Mettre en œuvre le processus de gestion de crise

08 Communiquer de manière contrôlée à l'extérieur / en interne

09 Notifier les autorités

10 Documenter la crise afin de conserver les preuves

APRÈS L'ATTAQUE

11 Documenter et organiser le retour d'expérience

12 Ré-évaluer les processus de gestion de crise

13 Communiquer sur les conséquences de l'attaque en interne

14 Réallouer des moyens à la sécurité en fonction du retour sur expérience

***AVERTISSEMENT** : ce document n'a pas vocation à être exhaustif, mais plutôt à contextualiser un sujet complexe sur la base des expériences croisées des participants à l'Atelier pour aider les opérationnels à convaincre leur direction des enjeux et de leurs besoins pour y répondre. Pour un approfondissement, il a été communément noté la qualité des guides hygiène et sécurité de l'ANSSI[1] et de la norme ISO 27001[2].*

[1] https://cyber.gouv.fr/publications/guide-dhygiene-informatique
[2] https://www.iso.org/fr/standard/27001

REMERCIEMENTS

Sous la direction de Corinne THIÉRACHE, Avocate Associée du Cabinet ALERION, en charge des Départements Propriété intellectuelle – Droit des Technologies et du Numérique - Protection des données personnelles et membre de la Commission juridique du GESTE, un atelier Cybersécurité a été lancé en novembre 2023 pour réunir les acteurs représentatifs des différentes catégories des médias en France entre novembre 2023 et juin 2024, afin de partager les expériences autour des cyberattaques déjà subies ou évitées (ci-après l' « Atelier »). A cette occasion, ont pu être dégagés des axes de recommandations à destination du secteur qui font l'objet de ce présent document (ci-après « Livre Blanc »).

Ont ainsi participé à cet Atelier :

- ALTICE GROUP : Matthieu HENNEBO (RSSI)
- BAYARD : Odile PICKEL (DPO interne)
- CMI FRANCE : Camille LANDRIEU (Directrice juridique), Anne GUILBERT (Responsable juridique) et Elise FONTAINE (Juriste)
- LE FIGARO : James BONNAVENTURE (RSSI)
- RADIO FRANCE : Margaux POUPART (Juriste RGPD)
- TELEGRAMME : Fabrice BOURGINE (DSI Groupe), Coralie FAVRESSE (Juriste RGPD)
- TF1 Le Groupe : Audrey COHAS (Responsable Juridique (IT / Assurances / Référent Data)
- TV5 MONDE : Yoann PAOLONI (RSSI)

Cet Atelier a en outre mobilisé l'expertise de Sébastien GANTOU, DPO externe et CEO du cabinet de conseil Digital DPO, membre du GESTE et de son groupe de travail de DPO depuis 2017.

DÉFINITIONS

CYBERATTAQUE

Ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.
Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée (Source ANSSI).

CYBERMENACE

Est un risque d'attaque de systèmes informatiques sur les infrastructures d'une compagnie, d'un Etat, d'une organisation privée ou publique, de son ou de ses systèmes d'information. Qu'ils soient isolés ou en réseaux et connectés ou non, les équipements visés peuvent être des ordinateurs, des serveurs, des imprimantes, des smartphones, des tablettes ou autres (Source ANSSI).

CYBERRISQUE

Tout risque de perte financière (pertes d'exploitations, et coût de remédiation), d'interruption des activités ou d'atteinte à la réputation d'une entreprise en raison d'une défaillance des systèmes de technologies de l'information.

CYBERSÉCURITÉ

État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberespace. La cybersécurité est assurée par la cyberprotection ainsi que, dans le cas d'un État, par la cyberdéfense (Source ANSSI).
Plus précisément cela vise l'état recherché pour permettre à un système d'information **de résister** à *des événements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* (Source ANSSI).

PLAN DE CONTINUITÉ D'ACTIVITÉ (PCA)

A pour objet de décliner la stratégie et l'ensemble des moyens humains, matériels et technologiques pour permettre à l'organisme de faire face à un sinistre informatique majeur et ainsi garantir la survie et la pérennité de ses activités pendant et après la survenue d'une crise, pour empêcher tout arrêt de l'activité.

PLAN DE REPRISE D'ACTIVITÉ (PRA)

A pour objet de gérer le risque en décrivant l'ensemble des procédures nécessaires à un redémarrage au plus vite du système d'information en définissant la nature et l'ordre des actions à mettre en place.

PHISHING

(Ou hameçonnage) est une technique de fraude en ligne où des cybercriminels se font passer pour des entités légitimes afin d'obtenir des informations personnelles sensibles des utilisateurs.

RANSOMWARE

(Ou rançongiciel) est un logiciel malveillant qui bloque l'accès à un ordinateur ou à des fichiers en les chiffrant jusqu'à ce qu'une rançon soit payée.

SYSTÈME D'INFORMATION

Ensemble des ressources internes ou externes — utilisateurs, outils, données — qui contribuent au traitement (numérique ou non) de l'information. Le système d'information est composé de trois types de ressources : l'outil informatique (infrastructure, matériel informatique, solutions applicatives ...), l'homme qui réalise une tâche avec ou sans l'outil, l'information qui représente la « matière première » (Source : Cairn informatique, numérique et système d'information : définitions, périmètres, enjeux économiques / Cairn.info).

RÉSUMÉ ANALYTIQUE ET CONTEXTUALISATION

Le monde des médias, englobant presse écrite, digitale et audiovisuelle, est particulièrement exposé aux cyberattaques, menaçant l'expression pluraliste des idées et la liberté fondamentale de l'information. Les risques cyber sont accentués par l'adoption croissante des technologies avancées et l'intégration poussée des systèmes d'information entre eux, en sus du recours à l'intelligence artificielle. Pour cette raison, ils sont désormais systémiques et augmentent la vulnérabilité des médias. L'importance des médias dans le tissu social et politique nécessite une attention accrue à leur protection contre ces menaces.

La question qui est la vôtre est donc la suivante : **« Le risque cyber évolue à la hausse tant en termes de probabilité d'occurrence qu'en termes d'impact opérationnel et financier, à quel moment la bascule vers une attitude proactive deviendra-t-elle une nécessité dans mon organisation ? »**

Afin de vous aider à identifier les enjeux, les parties prenantes et les processus clés à mettre en place et/ou à actionner, ce Livre Blanc vous est proposé par un groupe de travail dédié du GESTE, composé de membres de vos équipes et d'experts familiers des médias, reconnus parmi vos représentants habituels sur ces sujets.

Cet ouvrage comprend un retour d'expérience de plusieurs experts médias, exposant une situation réelle rencontrée ou partageant leurs bonnes pratiques éprouvées.

Quelques chiffres pour vous aider à prendre conscience des enjeux de la cybersécurité :

À l'échelle mondiale **et particulièrement pour le secteur des médias**, IBM évalue qu'en moyenne, une fuite de données coûtait 3,58 millions de dollars[3] à un média en 2023 (cf. graphique ci-dessous), contre 3,15 millions[4] en 2022.

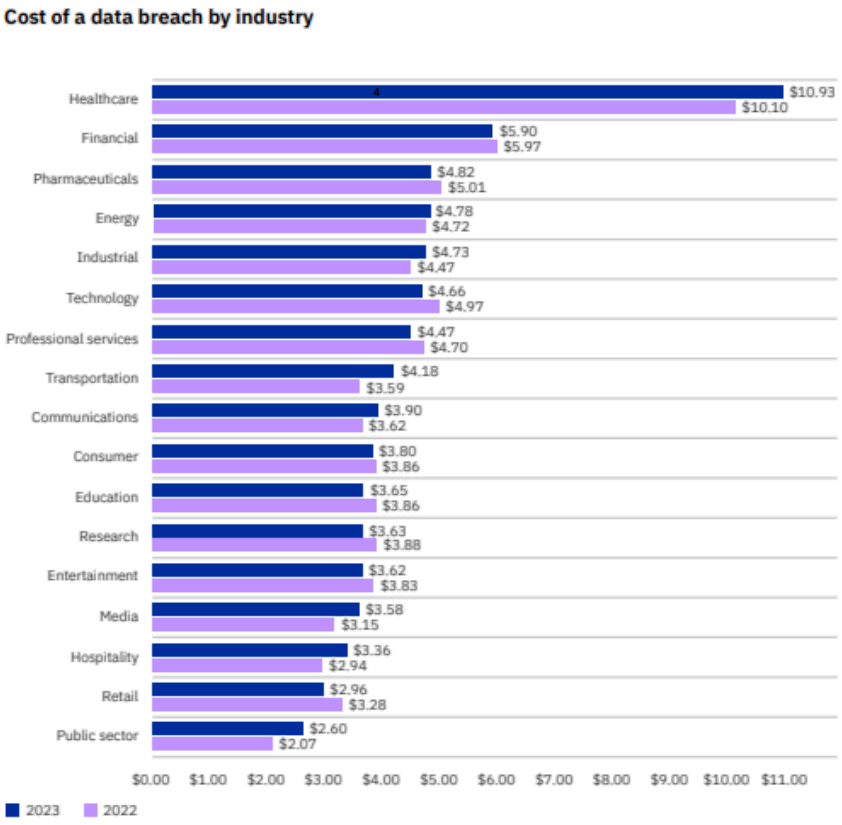
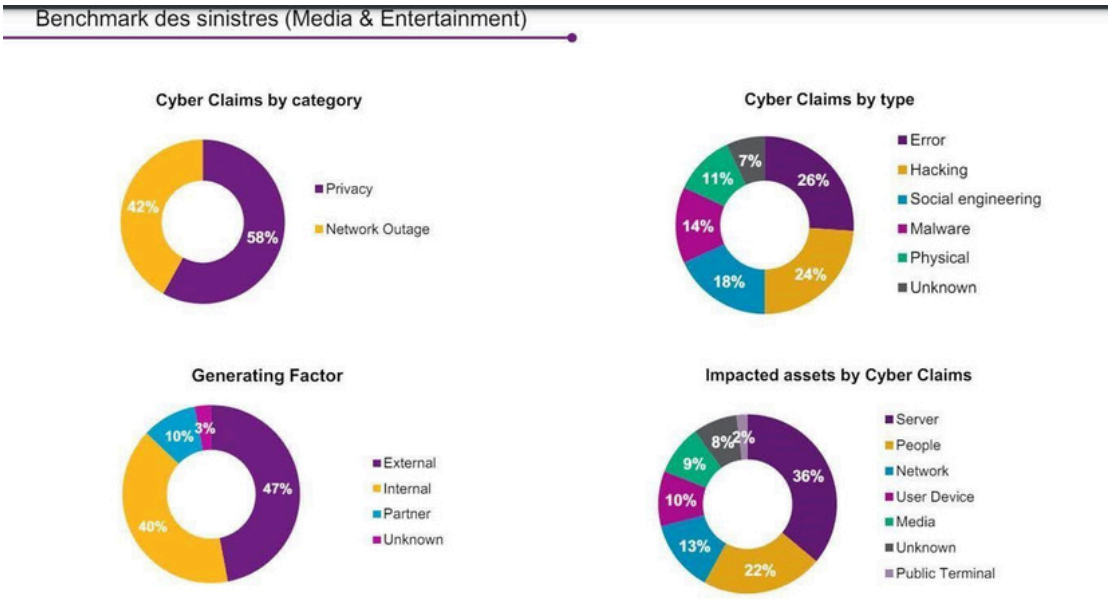


Figure 4. Measured in USD millions

Source : IBM, Cost of a Data Breach Report 2023, IBM Security (Graphique 4)

[3] Soit 3,3 millions d'euros environ selon le taux de change de mars 2024.
[4] Soit environ 2,9 millions d'euros selon le taux de change de mars 2024.



Source : Etude 2020 Willis Towers Watson

Le profil du sinistre type dans le secteur des médias est principalement composé d'incidents liés aux données, le fait générateur le plus commun étant l'erreur humaine. Le coût moyen constaté est de €2,9 M en 2019.
Les incidents impactent presque 1 fois sur 3 les serveurs et la principale cause génératrice est externe.

Le Livre Blanc s'articule autour de trois axes principaux en fonction de la phase dans laquelle se trouve l'organisation face à une cyberattaque. Le préambule positionne les enjeux, les parties prenantes et leur rôle respectif dans le processus.

PARTIE I - LES MESURES PRÉVENTIVES AVANT TOUTE CYBERATTAQUE

Tout d'abord, réaliser une analyse approfondie de l'activité

Les médias doivent réaliser une analyse minutieuse de leurs activités numériques pour identifier les actifs les plus critiques et exposés.

Cette analyse, basée sur l'impact qu'aurait un scénario catastrophe sur la vie de l'entreprise, aidera à prioriser des actions structurelles pour améliorer l'existant (travail des équipes, imbrication des processus ou moyens en place), à anticiper les risques et à élaborer une stratégie de gestion de crise adaptée pour protéger les actifs les plus précieux, ce qui suppose la détermination en amont des critères d'appréciation de la criticité et de la sévérité.

Ensuite, mettre en place des mesures techniques dites « de barrage »

Les mesures préventives sont diverses : il faudra veiller à leur rapport bénéfice/risque car elles impliqueront très probablement des changements sur la gestion ou l'accès à certaines données. Elles peuvent comprendre l'authentification forte, la mise en œuvre de politiques de mots de passe robustes, le changement des paramètres par défaut sur les équipements, et l'utilisation sécurisée des réseaux Wi-Fi et de l'Internet.

Techniquement, un élément crucial identifié par le groupe de travail est de sécuriser les réseaux en créant des cloisonnements entre les différentes zones du système d'information pour contenir les dommages.

Des référentiels de mesure auprès de l'ANSSI ou normes ISO 27001 peuvent être également très utiles pour identifier et mesurer les actions préventives à mettre en place. À ce titre, elles sont des références pertinentes pour mener un audit préventif de l'état des lieux.

Puis, instaurer des mesures organisationnelles pour préparer les équipes

La création d'un Comité Cybersécurité identifiant les responsables du pilotage en cas de crise avec les fonctions associées (Responsable de la Cybersécurité, RSSI, DPO, Communication, Juriste…) est primordiale et doit aller de pair avec l'élaboration d'un protocole de gestion de crise, régulièrement mis à jour et communiqué aux personnes concernées.

En cas d'incident impactant la disponibilité d'un ou plusieurs services, la mobilisation de l'ensemble des collaborateurs sera probablement progressive. Un plan de continuité et/ou de reprise d'activité doit/doivent être prêts et activables.

Il est essentiel de former et sensibiliser tous les employés à chaque niveau (y compris le top management) aux risques cyber. La formation doit être continue, pour augmenter la maturité des équipes, mais aussi ponctuelle et ciblée, avec des protocoles de crise et une anticipation de la mobilisation de l'ensemble des collaborateurs, pour une réponse rapide et efficace en cas d'incident. Ces considérations s'étendent également aux sous-traitants et aux fournisseurs. L'enjeu est également de maintenir à jour les connaissances en la matière (les techniques d'attaques évoluent), poursuivre les efforts en commun (accompagner les nouveaux collaborateurs - "onboarding" cyber).

Cela nécessite notamment d'avoir identifié des éléments de langage et des moyens de communication pouvant eux-mêmes être en dehors du système d'information adaptés à des scénarios de crise anticipés et adaptés en fonction de la criticité de l'impact et des populations concernées. Certains acteurs des médias vont notamment jusqu'à préparer des trames types en ce sens pour, le moment venu, être d'ores et déjà opérationnel (communication des salariés, utilisateurs, dépôt de plainte …).

L'organisation d'exercices de gestion de crise est un moyen efficace pour maintenir une bonne résilience.

Et enfin, prendre en compte les mesures juridiques et réglementaires impératives.

Les médias doivent être informés des législations et des délais applicables (RGPD, loi LOPPSI, Directive NIS 1...), ou en voie de l'être, telles que la Directive NIS 2, et la loi SREN – adoptée le 10 mars 2024, sous réserve d'avoir vérifié leur éventuelle soumission, au regard de leurs obligations en termes de cybersécurité.

Ils doivent étudier rationnellement le rapport coût/bénéfice d'une assurance sur le sujet cyber. Par ailleurs, il conviendra de s'assurer de la conformité aux réglementations de protection des données ou à celles applicables aux moyens de paiement – par exemple – afin de renforcer leur cybersécurité.

PARTIE II - LES MESURES PENDANT L'ATTAQUE

Mobiliser le protocole de gestion de crise

Une fois l'attaque détectée, il est crucial de mettre en œuvre immédiatement le protocole de gestion de crise, qui inclut des mesures techniques pour identifier et contrer l'attaque, ainsi que des mesures organisationnelles pour maintenir les opérations d'activité s'il existe, minimiser les dégâts, coordonner et tracer les actions de tous les intervenants pour ensuite pouvoir les documenter en vue de l'établissement de preuves.

En cas d'impact significatif sur les activités, le plan de reprise d'activité doit être activé.

Se conformer aux exigences réglementaires et légales

Il faut rapidement informer les autorités compétentes, telles que la CNIL[5] et l'ANSSI, et suivre les contraintes légales pour les notifications de violation de données et les plaintes auprès d'un service de police judiciaire générale ou spécialisée dans la lutte contre la cybercriminalité (BEFTI). Si vous disposez d'une assurance "Cyber", il sera nécessaire de déposer plainte sous 72H à compter de la connaissance de l'attaque pour activer vos garanties.

Ne pas négliger l'importance de la communication interne et externe

Selon les données concernées et l'impact sur la diffusion de l'information et/ou le respect des engagements publicitaires, un plan de communication opérationnel qui aura dû être préparé en amont devra être respecté pour application auprès des tiers concernés (clients, fournisseurs, abonnés), ce qui n'exclut pas des adaptations de dernière minute si nécessaire.

[5] Commission Nationale de l'Informatique et des Libertés

PARTIE III - LES MESURES APRÈS L'ATTAQUE

Une nécessaire gestion des conséquences

Après une cyberattaque, il est vital de communiquer efficacement à la fois en interne et en externe sur les raisons et les conséquences de l'attaque, en fonction de la situation, pour maintenir la confiance et la transparence avec les parties prenantes.

Il faut aussi analyser les échecs et les succès dans la gestion de l'incident pour améliorer la défense des actifs, la résilience de l'organisation et adapter les processus et protocoles internes.

Une amélioration continue à mettre en place

Les médias concernés doivent tirer des leçons de l'incident pour renforcer leur résilience à de futures attaques. Cela implique des ajustements dans les mesures techniques, organisationnelles et juridiques basées sur l'expérience acquise, le retour à un état de l'art ou la recherche d'une conformité homologuée ou certifiée et de mettre à jour le protocole de gestion de crise en conséquence. Il est impératif de documenter tout le processus et les mesures mises en place à la fois pour la conformité et la mémoire de l'entreprise.

CONCLUSION

La cybersécurité dans le secteur des médias n'est pas seulement une nécessité technique mais un impératif stratégique qui exige un engagement à tous les niveaux de l'organisation.

Il est essentiel que les directions des médias comprennent les enjeux et puissent agir en conséquence.

La sécurité numérique est cruciale pour la protection de vos actifs informationnels et votre capacité à servir la société démocratiquement.
Elle peut également vous permettre de protéger vos actifs et leur valeur pour vos actionnaires.

NOS DÉVELOPPEMENTS POUR APPROFONDIR

Pour une meilleure compréhension des risques et des bonnes pratiques à mettre en place

PRÉAMBULE

Le sujet du pluralisme des médias, qu'ils soient écrits, digitaux ou audiovisuels (presse écrite, radio, télévision ...), agite les esprits et réveille la nécessité de voir préserver la diversité des idées et des opinions. Toutefois, certains risques pouvant remettre en cause ce droit et cette liberté fondamentale pour toute société démocratique ne sont pas suffisamment pris en compte : les cyberrisques, conséquences de l'immersion de plus en plus importante des médias dans l'environnement numérique ou le cyberespace, qui sont par nature systémiques. La numérisation croissante, l'interconnexion des systèmes d'informations, l'émergence récente de l'Intelligence artificielle générative dans les médias (cf partenariat signé entre Le Monde et ChatGPT) sont des illustrations de cette exposition de plus en plus grande aux risques, amplifiée par le recours à de la technologie de plus en plus sophistiquée dans le secteur des médias, ce qui ne fait qu'exposer les actifs numériques concernés à des risques nouveaux, on parle de la surface d'une potentielle cyberattaque.

I. OBJECTIFS POURSUIVIS PAR LE LIVRE BLANC DU GESTE

En élaborant une cartographie des enseignements tirés d'un partage d'expérience entre les acteurs, membres du GESTE, ce Livre Blanc a pour objectif de mettre en commun ces bonnes pratiques pour en tirer des recommandations particulières à l'attention des organes de direction.

II. ENJEUX

- **La situation des médias face aux cyberattaques**

Les cyberattaques peuvent perturber voire empêcher la bonne diffusion des contenus produits par les médias : **c'est donc un sujet stratégique par nature**. Malheureusement, ces cyberattaques peuvent être facilitées en l'absence de réelle prise de conscience, au niveau des dirigeants, des actionnaires et des investisseurs, des enjeux liés à la cybersécurité.

Ce constat est d'autant plus inquiétant que, à grande échelle, la cyber malveillance est susceptible de mettre en déroute la diffusion d'informations d'intérêt public ou de mettre en péril des groupes de médias primordiaux, au risque de voir émerger ou prospérer des services de médias alternatifs concurrentiels aux contenus pouvant être moins sourcés, moins fiables ou moins vérifiés.

Pour dresser un bref tableau de la cyber malveillance, le cabinet d'études, de recherche et de conseil économique Asterès évaluait dans un rapport publié en 2023[6] à 2 milliards d'euros le coût des cyberattaques réussies sur les systèmes d'information des organisations françaises, toutes méthodes comprises, prenant ainsi en compte le coût de résolution de la crise, le coût moyen d'une rançon (lorsque rançon il y a) et les pertes moyennes de productivité.

[6] Asterès, *Le coût des cyberattaques réussies en France*, juin 2023

Plus récemment, IBM Security estime dans son rapport annuel sur les coûts des fuites de données[7] qu'une entreprise française subissait en 2023 en moyenne une perte de 4,45 millions de dollars[8], à la suite du vol, de la fuite ou encore de l'exfiltration de données.

L'expérience démontre que les pertes d'exploitation et les coûts de remédiation à la suite d'une cyberattaque sont en général bien plus élevés que les coûts représentés par une prévention et son évolution progressive.

- **La spécificité des médias face à des cyberattaques de masse ou ciblées**

  - **Des risques particuliers dus à l'intérêt général poursuivi par l'activité médiatique**

Au-delà des fuites de données, le constat du danger cyber grandissant subi par les médias est corrélé par les observations de l'ANSSI dans son Panorama de la cybermenace de 2023 où elle constate un « *regain du nombre d'attaques destinées à promouvoir un discours politique, à entraver l'accès à des contenus en ligne ou à porter atteinte à l'image d'une organisation* ». Elle ajoute que ces actions de déstabilisation se sont principalement manifestées sous la forme « *d'attaques par déni de service distribué (DDoS)*[9] *conduites par des groupes d'hacktivistes pro-russes très réactifs à l'actualité, mais dont les impacts restent limités* ». L'ANSSI ne manque pas non plus de souligner avoir eu connaissance de la compromission d'une partie du système d'information d'un *média français qui a abouti à la divulgation d'informations exfiltrées en représailles à de précédentes publications*.

Cela rejoint finalement la déclaration faite par l'agence nationale à l'occasion de l'attaque informatique qui avait touché TV5 Monde en 2015 ; l'ANSSI affirmait alors déjà que cette attaque s'inscrivait *« dans le contexte d'une guerre de l'information où les médias sont particulièrement visés, ainsi que plusieurs incidents récents l'ont confirmé : il s'agit, pour les attaquants, d'une méthode de propagande*[10] ».

L'analyse du contexte géopolitique est en effet primordiale à la bonne compréhension des risques cyber touchant particulièrement les médias. Les enjeux politiques, les conflits militaires, les élections importantes dans le monde, les crises sanitaires ainsi que les évènements internationaux doivent être pris en compte. De manière générale, la gravité des répercussions qu'occasionnerait la déstabilisation des médias via des cyberattaques (exfiltration de données, mise en déroute des systèmes d'information, etc.) est alarmante, sans parler de l'atteinte à la réputation dudit média. Ceci dans le contexte de sensibilité voire de fragilité de l'information.

[7] IBM, Cost of a Data Breach Report 2023, IBM Security.
[8] Soit environ 4,10 millions d'euros en 2024.
[9] Distributed Denial of Service attack : rendre indisponible un service par l'envoi de multiples requêtes originaires de plusieurs sources.
[10] ANSSI, Attaque informatique contre TV5 Monde : l'ANSSI mobilisée, Communiqué de presse, 9 avril 2015.

La très récente immersion au cœur des médias de l'intelligence artificielle pourtant facteur de risques de lourdes failles de cybersécurité (divulgation d'informations, inclusion d'un vaste système extérieur dans le système interne)[11], en tout état de cause à des fins pécuniaires, souligne encore davantage la nécessité pour les services de médias de prendre conscience des risques cyber encourus et le besoin pressant d'acquérir des réflexes primordiaux de cybersécurité.[12]

Si les médias subissent bien des cyberattaques chaque jour, comme d'autres secteurs, ces dernières concernent soit des fuites de données sans réel impact immédiat sur l'activité des médias qui peuvent continuer à diffuser, soit des intrusions suffisamment graves dans le système d'informations pour empêcher notamment une chaîne de télévision d'émettre et la réduire au silence (plus de sons, plus d'images avec les conséquences graves en matière d'obligations au regard de l'attribution des ressources) à la suite de récupération des identifiants des systèmes de réseaux, des réseaux sociaux ainsi que du service de messagerie. Dans ce dernier cas, l'objectif de l'attaque étatique ciblée est clair : détruire la chaîne (sans demande de rançon), atteindre l'image de la France.

- **Des types d'attaques et la nature singulière des données dont les médias sont dépositaires**

Une observation demeure : comme la plupart des fournisseurs de services, les médias sont l'objet d'une grande diversité d'attaques qui cherchent tout aussi bien à les atteindre par l'extérieur (notamment par *typosquatting* ou typosquattage)[13] que par l'intérieur (par exemple via un logiciel de type *Crypto Locker, logiciel qui chiffre les données et les accès empêchant toute utilisation du système d'information concerné*), tant pour mettre en danger l'activité du média qu'à des fins d'extorsion financière (par des manœuvres telles que le *phishing* – ou hameçonnage - et les arnaques au président).

Ces attaques peuvent ainsi être réparties entre trois grands risques encourus par les médias :

- L'attaque visant les actifs digitaux par ransomware ;
- L'attaque avec impact opérationnel par DDOS ou par le simple blocage des outils éditoriaux voire de l'accès à l'ensemble des services ;
- L'attaque préparée à l'avance des comptes des salariés à l'aide de l'ingénierie sociale (manipulation psychologique à des fins d'escroquerie) par les tentatives de phishing à l'occasion des grands évènements tels que le Black Friday[12] ou les Jeux olympiques ;

Réalisées lors de périodes critiques de vacation de la majorité des employés de la structure (Vacances de Noël et weekends), la plus simple des attaques peut prendre une ampleur démesurée.

[11] On pense notamment à la conclusion d'un partenariat entre Le Monde et OpenAI permettant au second de puiser ses données dans les articles du soir du Monde en contrepartie de l'accès de ce dernier à son système d'intelligence artificielle générative.

[12] Pour mémoire : Norme ISO 38507 traitant des implications de gouvernance dans l'utilisation de l'IA par des organisations et Recommandations de sécurité l'ANSSI pour un système d'IA générative.

[13] Attaque visant les internautes tapant incorrectement une URL dans leur navigateur Web.

Il est fréquent que les informations détenues par les médias soient la cible des cyber attaquants, leur spécificité leur conférant une valeur intrinsèque facilement valorisable pour un tiers malveillant. Les fournisseurs de médias sont en effet dépositaires à la fois de données financières et confidentielles classiques à tout type de société, et à la fois de données beaucoup plus sensibles telles que des données personnelles à grande échelle, des données pouvant dévoiler des opinions politiques et des données journalistiques. Ces données journalistiques sont la matière précieuse du secteur qu'il convient de protéger à tout prix dans la mesure où leur divulgation serait susceptible de compromettre les sources des journalistes qui bénéficient d'une protection particulière (article 2 de la loi du 29 juillet 1881), tout comme les enquêtes journalistiques en cours sur des sujets d'information potentiellement explosifs, voire de mettre en danger certaines personnes protégées (par exemple des reporters sous identité cachée). Il n'est ainsi pas rare que certaines données relatives à des sujets d'enquête d'investigation particulièrement brûlants fassent l'objet d'attaques ciblées destinées à les exfiltrer. Dans ce cadre, il est essentiel d'identifier les profils à risques qui manipulent ces données critiques (personnelles, stratégiques, confidentielles ...).

- **Les organes de direction des médias, décisionnaires de la Cybersécurité**

Le double objectif de la cybersécurité est :

01

La formation et la sensibilisation de tous les acteurs aux risques cyber et aux bonnes pratiques avec une hygiène informatique à mettre en œuvre au quotidien pour prévenir la survenance et les coûts des cyberattaques.

02

L'acquisition de solutions techniques pour protéger les données et les services informatiques et permettre la continuité des services pour être capable de poursuivre en mode dégradé (plan de continuité et plan de reprise d'activité).

La réalisation de cet objectif suppose l'attribution de moyens humains et financiers à la hauteur des enjeux et des risques.

A ce titre, la cybersécurité doit être une préoccupation constante non seulement des équipes techniques (DSI, RSSI, ingénieurs informatiques), des équipes juridiques (Directeur et Responsable juridique, DRH), des DPO, mais également et surtout, en tant que décisionnaires, des dirigeants, des investisseurs et des actionnaires qui définissent les priorités, arrêtent les budgets et sont à même de mobiliser l'ensemble d'une entreprise.

La cybersécurité est un sujet dont doivent se saisir les COMEX ou conseils d'administration en lien avec la sûreté des outils afin d'adresser cette problématique comme étant prioritaire, favoriser la prise de conscience à tous les niveaux et attribuer les budgets nécessaires. La maturité sur le sujet souffre le plus souvent de méconnaissance des risques et des enjeux, et de l'absence de mobilisation des moyens financiers humains et techniques compte tenu des coûts. Il s'agit certes d'investissements mais qui aboutissent à de la création de valeur à la fois financière, patrimoniale, réputationnelle, humaine de l'entreprise.

Il appartient donc aux organes de direction des services de médias de prendre en compte la cybersécurité dans leur plan de développement pour assurer une performance pérenne, résiliente et sécurisée à l'aide notamment de savoir-faire développés dans la gestion de crise.

III. IDENTIFICATION DES PARTIES PRENANTES

- Direction Générale
- RSSI (Responsable de la Sécurité des Systèmes d'Information) ou à défaut DSI, CIO ou responsable identifié de la cybersécurité
- DPO (Data Protection Officer)
- Direction Juridique (juristes et/ou avocats) et personnes en charge des assurances cyber
- Équipe IT/DSI
- Prestataires externes (sécurité informatique, consultants)
- Équipe de communication
- Cellule de crise

Composition type de la cellule de crise

- RSSI : Responsable de la sécurité des systèmes d'information
- Equipe IT : Directeur ou Responsable des systèmes d'information
- DPO : Data Protection Officer
- Responsable de communication
- Prestataires externes : Experts techniques et sous-traitants selon l'incident
- Conseiller juridique dont les avocats (pour les implications légales des incidents)
- Selon l'incident, représentant de la Direction

Les rôles et responsabilités des parties prenantes (RACI) sont explicités en Annexe 2 des présentes.

IV. SYNTHÈSE DES PLANS D'ACTIONS SOUS FORME DE FRISE CHRONOLOGIQUE

AVANT LA CYBERATTAQUE	DURANT LA CYBERATTAQUE	APRES LA CYBERATTAQUE
Cartographier ses actifs et analyser les risques et leurs impacts	Mesurer l'impact de l'attaque et Isoler les actifs concernés	Documenter et organiser le RETEX
Allouer des moyens à la sécurité, mise en place de mesures adaptées (Interne et Sous-traitants)	Mettre en œuvre le processus de gestion de crise	Ré-évaluer les processus de gestion de crise
Adopter un dispositif de gestion de crise en nommant un comité de gestion de crise	Communiquer de manière contrôlée à l'extérieur / en interne	Communiquer sur les conséquences de l'attaque en interne
Former les équipes et les dirigeants	Notifier les autorités	Ré-allouer des moyens à la sécurité en fonction du retour sur expérience
Se faire auditer et s'entraîner en simulant une crise pour tester la task force de crise	Documenter la crise afin de conserver les preuves	

Digital DPO 2024, Ateliers GESTE - Cybersécurité et Médias

Nos recommandations sont organisées dans le présent document autour de 3 axes principaux synthétisant, de manière chronologique au cours des différentes phases de la cyberattaque :

- Les mesures à mettre en oeuvre préventivement à toute cyberattaque (Partie I)
- Celles qui doivent être déclenchées en cours de cyberattaque (Partie II)
- Et enfin celles à envisager à la suite d'une cyberattaque (Partie III)

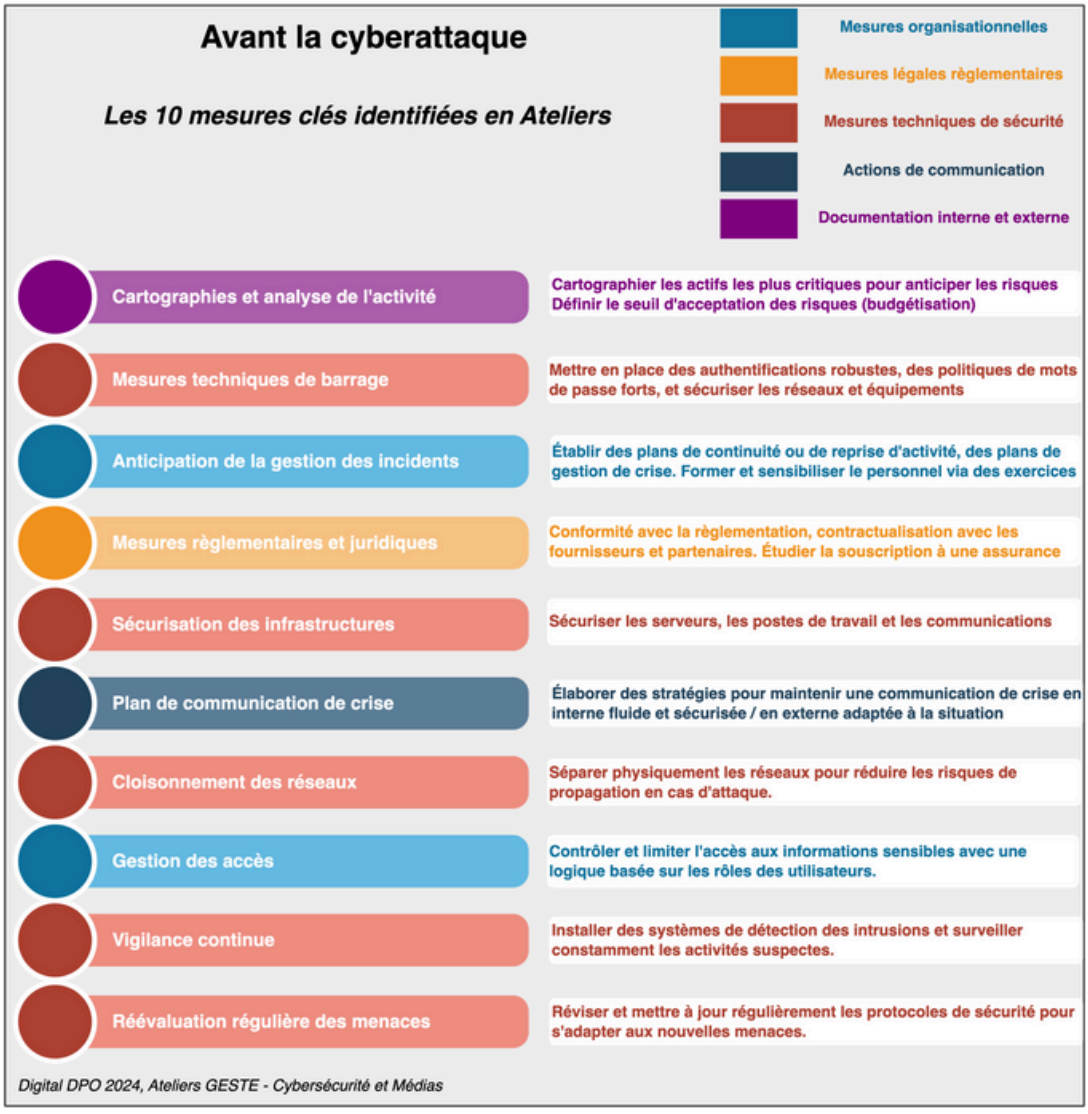
« *se préparer au pire pour donner le meilleur*[14] »

[14] *Crise Cyber : se préparer au pire pour donner le meilleur, de Sébastien Jardin & Stephen Delahunty (Édition Mars 2024 PEARSON)*

PARTIE I - LES MESURES PRÉVENTIVES AVANT TOUTE CYBERATTAQUE

La prévention est le premier pilier de la cybersécurité : elle est incontournable pour tout média qui cherche à s'économiser à l'avenir des frais démesurés de gestion de crise de cyberattaque qui auraient pu être limités par un investissement préalable dans des mesures techniques (2), organisationnelles (3) et juridiques (4) efficaces. L'analyse d'un cas concret permettra de mettre ce constat en évidence (5).

La mise en place de ces mesures doit toutefois être précédée d'une analyse poussée de la structure du fournisseur du médias (1).



1 ANALYSER EN PROFONDEUR SON ACTIVITÉ EN DRESSANT LA CARTOGRAPHIE DES ACTIFS LES PLUS CRITIQUES, LES PLUS STRATÉGIQUES ET LES PLUS EXPOSÉS

La première étape, et certainement la plus importante de toutes, pour toute entité cherchant à développer sa cybersécurité : la bonne compréhension de son activité numérique. Il est ainsi nécessaire d'identifier les actifs les plus critiques, les plus stratégiques et les plus exposés aux dangers du numérique.

- Dans le cas d'un fournisseur de média exploitant les technologies du numérique pour son activité, les bases de données documentaires, les dossiers de recherches et les données concernant des personnes physiques protégées (sources journalistiques, reporters d'investigation) sont autant d'actifs incorporels qu'il est impératif de protéger.

- De même, les données bancaires traitées à grande échelle pour les paiements en ligne des abonnements numériques ou pour les paiements à distance des abonnements traditionnels qui sont gérés le plus souvent par une chaîne de sous-traitance externe.

Il est ensuite nécessaire pour les dirigeants d'un service de médias ou, le cas échéant, la personne en charge d'une telle responsabilité, de déterminer son seuil d'acceptation des risques afin de pouvoir envisager la proportion de ses investissements liés à la cybersécurité face à son immersion dans ses activités numériques. Cela lui permettra de construire les « pires scenarii » possibles aux fins d'identification des situations critiques et d'estimer, pour chacune, les pertes financières probables, leur niveau de gravité et leur vraisemblance.

Plus encore, il lui sera ensuite possible de **définir une stratégie de sécurité numérique et de valorisation** déterminant les choix prioritaires de protection de l'entreprise en termes de plan d'intégration de la cybersécurité mais également en cas de cyberattaque.

- Pour les services de médias, ce choix prioritaire pourrait porter sur le maintien de la diffusion des contenus éditoriaux, coûte que coûte, à faire figurer dans le plan de continuité d'activité.

À ces choix seront donc allouées des ressources et un plan constitué d'étapes permettant de tracer la voie jusqu'au niveau de cybersécurité souhaité. Ces étapes impliquent une analyse approfondie des risques encourus par l'entité, la définition d'une stratégie (implémentation progressive d'une politique de sécurité des systèmes d'information (PSSI) et la mise en place d'un plan d'amélioration continue de la sécurité (PACS).

L'ensemble de ces investissements en cybersécurité peut par ailleurs être valorisé par le biais de l'homologation qui permet de garantir que la structure est consciente des risques cyber qu'elle encourt et qu'elle les maîtrise. L'ANSSI a publié en 2017 à ce sujet un guide de neuf étapes.[15]

[15] *L'homologation de sécurité en neuf étapes simples, ANSSI, 2017, www.ssi.gouv.fr/guide-homologation-securite*

2 METTRE EN PLACE DES MESURES TECHNIQUES FAISANT BARRAGE AUX CYBERATTAQUES

Ces mesures préventives techniques, si elles s'adressent davantage au personnel employé en charge de la sécurité des systèmes d'information du média, sont primordiales et doivent être également connues des organes de direction des services de média, même imparfaitement.

Instaurer des mesures techniques permettant de faire obstacle à d'éventuelles cyberattaques implique tout d'abord de mettre en place des procédures d'authentification minutieuse, une charte de l'utilisateur du SI et des comptes à hauts privilèges, rappelant la responsabilité des administrateurs et un contrôle des accès infaillibles : il est nécessaire d'identifier chaque personne accédant au système et d'avoir une approche nominative permettant de distinguer le simple utilisateur de l'administrateur. Cela permettra par la suite d'attribuer à chacun des droits d'accès correspondants à son niveau de responsabilité et au niveau de sensibilité des données.

- Pour un média en ligne par exemple, s'il est légitime que le directeur des publications ait accès à l'ensemble des données de recherche, cela l'est moins pour un chroniqueur occasionnel, un pigiste ou un stagiaire.

Ces accès doivent ensuite être protégés par une politique forte et précise sur les mots de passe : il est impératif de mettre en place des bonnes pratiques en matière de choix et de dimensionnement de mots de passe puis de protéger ces mots de passe lorsqu'ils sont stockés sur le système.

À cet effet, il convient de se conformer aux recommandations de la CNIL et de l'ANSSI en la matière qui évoluent avec le temps compte tenu de la grande agilité des cyber attaquants.

Toujours dans cette optique de protéger le système des intrusions indésirables, changer les éléments d'authentification par défaut sur les équipements et services est primordial tant les éléments installés par défaut peuvent être triviaux ; il convient à l'inverse de privilégier et généraliser une authentification forte dès que cela est possible à deux facteurs.

Au-delà ensuite, classiquement, de la sécurisation des postes (sécurité minimale sur l'ensemble du parc informatique, restriction de l'usage des supports amovibles, utilisation d'un outil de gestion centralisé et chiffrement des données transmises par Internet), il est nécessaire pour le service de médias qui cherche à se prémunir contre les cyberattaques de sécuriser son réseau. À cette fin, et dans l'optique de bâtir une protection numérique, il est nécessaire de mettre dans un premier temps en place un cloisonnement entre les zones de réseaux en regroupant distinctement « les serveurs d'infrastructures des serveurs métiers, des postes de travail utilisateurs, des postes de travail administrateurs, des postes de téléphonie sur IP, etc. »[16]

[16] ANSSI et AMRAE, Maîtrise du risque numérique : L'atout confiance

Il est dans un second temps nécessaire de s'assurer de la sécurité des réseaux d'accès Wi-Fi et du processus BYOD notamment par un chiffrement robuste (mode WPA2 dans l'attente de la version WPA3, algorithme AES CCMP) et de la séparation des usages professionnels et privés, en veillant à être toujours à jour des normes de chiffrement. Pour ce qui est de l'usage des réseaux, il est ensuite nécessaire d'utiliser des protocoles de réseaux sécurisés (les protocoles les plus courants reposant sur l'utilisation de TLS 1.2 et au-delà), de même que pour l'accès à internet pour lequel il convient d'utiliser un protocole sécurisé comprenant au minimum un pare-feu pour filtrer les connexions et un serveur mandataire (proxy) en bannissant des protocoles d'administration non sécurisés (ex : Telnet, VNC) et d'échanges de fichiers (ex : SMBv1, FTP). Cela passe aussi par un travail acharné et difficile auprès de certains éditeurs/fournisseurs pour imposer et faire accepter ces standards incontournables. Le cadre contractuel évoqué ci-après peut aider à cet égard (Plan Assurance Sécurité).

Enfin, la protection de la messagerie professionnelle est un mécanisme primordial à mettre en place (spam, vérification d'authenticité, avec la définition du niveau de confidentialité des données manipulées et échangées (DLP : Data loss prevention), procédure de signalement de tout mail suspicieux pour les utilisateurs), d'autant plus lorsqu'on considère que les fuites de données journalistiques proviennent dans la majorité des cas d'un défaut de protection à ce niveau. Le recours à des outils de chiffrement est également une autre solution pour des données spécialement sensibles.

Il est recommandé de faire procéder, dans un cadre contractuel bien défini avec les obligations de chacun, à des tests d'intrusion pour s'assurer de l'absence de vulnérabilités.

Enfin, il faut souligner l'importance des barrières de protection physique. Une bonne maîtrise des accès aux locaux et la mise en place d'un système d'alerte en cas d'intrusion sont des moyens de limiter les voies d'action des cyberattaquants. De même, interdire l'accès à Internet depuis les postes ou serveurs utilisés pour l'administration du système d'information et imposer pour ce dernier l'utilisation d'un réseau dédié et cloisonné permettrait de diminuer de manière importante les risques d'exposition du système d'information principal. Ainsi, une règle simple : l'accès au réseau interne et externe doit être toujours authentifié. Ces bonnes pratiques ne doivent pas faire oublier le maintien de la sûreté de l'accès des lieux physiques, le matériel et l'immatériel cohabitant de plus en plus.

3 METTRE EN PLACE DES MESURES ORGANISATIONNELLES SPÉCIFIQUES

Mettre en place des mesures organisationnelles propres au service de médias en ligne signifie pour les organes de direction savoir mobiliser les ressources humaines existantes dont dispose l'entité pour réduire le plus possible le risque de cyberattaque mais également pour appréhender au mieux leur éventualité, et ainsi organiser l'entité de telle sorte qu'elle soit prête à réagir à une situation réelle (organiser la cyber résilience).

- **Formation et sensibilisation à tous les niveaux**

Cela signifie dans un premier temps mettre en place une sensibilisation initiale et continue des salariés pour prendre en compte le grand « facteur humain » de la cyberattaque.

La cybermalveillance repose autant sur des failles technologiques qu'humaines (ressorts d'ingénierie sociale). Les failles humaines peuvent être de plusieurs ordres : erreurs, malveillances, mauvais usages. Il est ainsi nécessaire de mettre en place des formations et des exercices fréquemment pour permettre au personnel employé au sein du service de médias d'acquérir les compétences nécessaires pour protéger l'entité et sa propre activité face aux cyberattaques mais également pour lui permettre de maintenir ses compétences et ses réflexes sur une base régulière au fil du temps. A ce titre, la mise à jour des formations doit faire partie des objectifs annuels des salariés. Dans la même logique, la sensibilisation des dirigeants n'est pas à négliger et doit absolument être prise en compte dans les formations à mettre en place, et ce d'autant plus que les dirigeants occuperont toujours une position de prise de décision — ou à tout le moins de validation de cette dernière - lors du déclenchement des cellules de crises en cas de cyberattaque.

- **Mise en place d'un scénario d'attaque simulés**

Pour renforcer la préparation des équipes, il est possible de mettre en place des scénarios d'attaque simulés. Ces exercices permettent de tester la réactivité des équipes face à des situations réalistes, d'identifier les points faibles des procédures existantes, et de former les collaborateurs à réagir efficacement en cas de cyberattaque. La simulation d'attaques de type ransomware ou d'autres menaces spécifiques aux médias peut révéler des vulnérabilités critiques avant qu'elles ne soient exploitées.

- **Création d'une task force et d'un comité cybersécurité**

Les mesures organisationnelles passent toutefois essentiellement par la création d'une task force, d'une cellule destinée à gérer les situations de crise. Cette task force devrait de manière générale avoir pour mission de définir un cadre de gouvernance du risque numérique. Il est possible de dresser un tableau théorique de la composition de cette task force en procédant par regroupement des compétences nécessaires à son fonctionnement : il serait ainsi nécessaire d'y inclure le DPO (Data Protection Officer), le DSI et le RSSI (Responsable de la Sécurité des Systèmes d'Information) du fournisseur de service de médias. Il faudrait également y inclure des membres des équipes techniques, financières, de communication, juridiques et des ressources humaines pour que la task force soit à même de créer des protocoles et politiques de cybersécurité parfaitement en adéquation avec la structure.
Par ailleurs, instaurer un comité cybersécurité et l'organiser de telle manière à ce qu'il puisse se réunir fréquemment afin de repenser les protocoles et politiques mises en place, notamment quant au plan d'amélioration continue de la sécurité (PACS) en fonction des nouveaux outils et des nouvelles pratiques des cyber attaquants connues grâce à une veille est un atout conséquent pour toute structure qui vise à se protéger face aux risques numériques sur le long terme. Ce comité cybersécurité aura notamment pour mission de repenser le protocole de gestion de crise imaginé par la task force afin de le faire évoluer.

Enfin, les exercices mis en place dans le cadre de la sensibilisation doivent impérativement inclure des simulations d'incidents réels afin d'éprouver les compétences acquises par l'ensemble des personnes travaillant au sein du service de média mais également pour tester la bonne marche de la procédure d'alerte et de gestion de crise.

- **Publication de contenus en mode dégradés**

Pour les médias, la continuité de la diffusion est essentielle, même en cas de cyberattaque sévère. Il est donc crucial de prévoir des stratégies de publication en mode dégradé, permettant de continuer à diffuser des contenus essentiels, même si les systèmes principaux sont compromis. Cela peut inclure l'utilisation de canaux alternatifs, des solutions de secours pour l'hébergement de contenu, ou des accords avec des partenaires pour garantir la continuité du service.

4 PRENDRE EN COMPTE LES MESURES JURIDIQUES IMPÉRATIVES

Comprendre et cerner son activité signifie également, pour les organes de direction des médias, avoir une appréhension claire du cadre légal et réglementaire applicable au numérique régissant cette activité.

Sur le cadre réglementaire d'ores et déjà en vigueur, il convient d'envisager en premier lieu le **Règlement Général sur la Protection des Données personnelles** (RGPD)[17]. Plusieurs articles de la réglementation intéressent directement la prévention des cyberattaques. Ainsi, l'obligation d'assurer la sécurité des données personnelles collectées (article 5 f. du RGPD) de même que l'obligation de minimiser cette collecte (article 5 c. du RGPD) ou encore de délimiter la conservation des données personnelles une fois collectées (article 5 e. du RGPD) cherchent à imposer aux responsables de traitement la mise en œuvre de mesures organisationnelles, techniques et juridiques minimum visant à prévenir toute cyberattaque ou, ad minima, à en limiter les éventuels dégâts. Pour rappel, une donnée personnelle s'entend de toute information se rapportant à une personne physique identifiée ou identifiable (article 1er du RGPD). De même, il convient d'avoir en mémoire les obligations de sécurité prévues à l'article 32 du RGPD incombant au responsable de traitement.

Dans le cas des médias en ligne, se pose notamment la question de **l'éventuelle applicabilité des Directives dites « NIS », soit NIS 1 et en particulier NIS 2.**[18]

La Directive dite « *Network and Information Systems 2* », NIS 2 ou encore SIR 2, adoptée le 14 décembre 2022, a en effet pour objectif d'assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union européenne en améliorant les capacités nationales en matière de cybersécurité, en renforçant la coopération au niveau de l'Union et en faisant la promotion d'une culture de la gestion des risques et du signalement des incidents parmi les principaux acteurs économiques.

[17] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), entré en vigueur le 23 mai 2018

[18] Directive (UE) 2022/2555 du Parlement européen et du Conseil, modifiant le Règlement (UE) n° 910/2014 et la Directive (UE) 2018/1972, et abrogeant la Directive (UE) 2016/1148

Au jour de l'élaboration de ce Livre Blanc, soit bien après l'entrée en application de NIS 1 mais avant la transposition en droit interne de NIS 2 - qui devrait entrer en vigueur avant le 17 octobre 2024 -, et selon la lettre du texte, la Directive NIS 2 ne serait pas applicable aux fournisseurs de services de médias en ligne. Les entités tombant sous le joug des obligations de cybersécurité renforcées prévues par NIS 2 ne comprennent en effet pas les médias en ligne.

La Directive inclut tout d'abord seulement dans les secteurs hautement critiques les « fournisseurs de services de communications électroniques accessibles au public » pour lesquels elle renvoie à une définition excluant expressément les « services consistant à fournir des contenus transmis à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus » (article 2 de la Directive (UE) 2018/1972 établissant le code des communications électroniques européen).

Ensuite, dans son champ élargi d'application, la Directive prévoit également dans ces secteurs hautement critiques la « *gestion des services TIC* » en n'y incluant toutefois que les « *fournisseurs de services gérés* » qu'elle définit comme des entités fournissant des « *services liés à l'installation, à la gestion, à l'exploitation ou à l'entretien de produits, de réseaux, d'infrastructures ou d'applications TIC ou d'autres réseaux et systèmes d'information, par l'intermédiaire d'une assistance ou d'une administration active, soit dans les locaux des clients, soit à distance* » (article 6 point 39) ce qui exclut également sans aucun doute les fournisseurs de services de médias en ligne.

La seule incertitude demeure sur la marge de manœuvre offerte aux États membres à l'occasion de la transposition de NIS 2, qui leur laisse la possibilité de prévoir des exceptions nationales en désignant toute entité « essentielle » ou « importante » qui serait essentielle « *au maintien d'activités sociétales ou économiques critiques* » ou critique « *en raison de son importance spécifique au niveau national ou régional pour le secteur ou le type de service en question, ou pour d'autres secteurs interdépendants dans l'État membre* » ou encore dans le cas où une « *perturbation du service fourni par l'entité pourrait avoir un impact important sur la sécurité publique, la sûreté publique ou la santé publique* ». Néanmoins ce recensement ne peut avoir lieu que dans le cadre strict des secteurs désignés par NIS 2, ce qui exclurait *in abstracto* les services de médias en ligne.

Par ailleurs, la possibilité pour les États membres d'établir, jusqu'au 17 juillet 2026, une liste d'« entités critiques » en vertu de la Directive 2022/2557 sur la résilience des entités critiques dite Directive CER laisse également une porte ouverte à la France pour inclure les services de médias en ligne (les « entités critiques » étant soumises aux mêmes obligations que les « entités essentielles » de NIS 2). Toutefois, la Directive 2022/2557 précise que les entités critiques désignées doivent entrer dans des secteurs correspondant en tous points à ceux de NIS 2. Tout comme la marge de manœuvre sur les entités « essentielles » et « importantes », la souplesse accordée sur les « entités critiques » ne permet donc a priori pas d'inclure les services de médias en ligne.

À date, un projet de loi relatif à la résilience des activités d'importance vitale, à la protection des infrastructures critiques, à la cybersécurité et à la résilience opérationnelle numérique du secteur financier ne permet malheureusement pas d'apporter une réponse claire à nos interrogations puisque beaucoup d'aspects sont renvoyés à la promulgation de futurs décrets.

La transposition de la Directive NIS 2 est donc à suivre de près, un référentiel sur la question devant être adopté très prochainement officiellement ;[19]

Dans le cas où les fournisseurs de services de médias en ligne se verraient être inclus au titre d'« exception nationale » dans les entités soumises à la Directive, ils bénéficieraient d'une période de transition de 2 à 3 ans à partir du 17 octobre 2024 avant qu'elle ne soit contraignante sur les obligations de cybersécurité renforcées[20] (audits obligatoires, sécurisation de la chaîne d'approvisionnement, gestion des risques par les dirigeants, obligations de notification des incidents à l'ANSSI, pouvoirs de sanction et de contrôle de l'ANSSI...).

Parmi les dispositions relatives aux sanctions, il est notamment prévu que celles-ci peuvent être également prononcées à l'encontre des dirigeants qui n'auraient pas justement accordé tous les moyens nécessaires notamment financiers pour assurer des mesures de cybersécurité.

En tout état de cause, un média sous-traitant d'un fournisseur de biens ou de services soumis à la Directive NIS 2 (services de communications électroniques accessibles au public, réseaux sociaux, moteurs de recherche, places de marché...) pourrait se voir répercuter les obligations de son cocontractant (contrôle de toute la chaîne d'approvisionnement).

Parmi les mesures juridiques à envisager, **le choix d'une police d'assurance adaptée pour les cyberattaques doit être considéré** : si les risques de subir une cyberattaque bloquante sont nettement diminués par la mise en place d'une politique de cybersécurité concrète, des préjudices sont toujours à déplorer. Transférer ce risque à une assurance soigneusement choisie permet de pallier cet impact financier. Il convient donc de faire l'inventaire des quelques couvertures existantes pour en ressortir la meilleure – et la plus adaptée à l'activité spécifique des médias en limitant les coûts parfois exorbitants de certaines polices – ce qui peut se faire par l'intermédiaire d'un courtier en assurances. A cet égard, il est recommandé de répondre de bonne foi au questionnaire de l'assureur, même si certains apparaissent orientés voire déconnectés de la réalité du terrain, pour ne pas se voir refuser le dédommagement. Parfois, il peut être choisi au contraire de ne pas reconduire son assurance cyber risques après une analyse approfondie de ce que cette dernière proposait réellement en termes de transfert de responsabilité.

Enfin, il convient de rappeler ici la nécessité de disposer d'une documentation de conformité appropriée. Au niveau interne, cette documentation couvre notamment les chartes informatiques, les règlements intérieurs, les codes de bonnes pratiques à destination des opérationnels.

[19] Informations délivrées par l'ANSSI au Forum InCyber de Lille du 26 au 28 mars 2024.
[20] Informations délivrées par l'ANSSI au Forum InCyber de Lille du 26 au 28 mars 2024.

Au niveau externe, cette documentation est tout d'abord contractuelle (vis-à-vis des fournisseurs de solutions, sous-traitants) rappelant, en sus de la nécessité du respect des règles en matière de protection des données personnelles, les règles relatives à la confidentialité et les mesures prises en matière de sécurité. Il est également recommandé d'inclure des questionnaires RGPD à destination des fournisseurs.

5 S'INSPIRER D'UN CAS CONCRET DE MISE EN PLACE DE MESURES PRÉVENTIVES

Le GESTE a eu l'occasion d'étudier les mesures mises en place par un groupe de médias préventivement à toute cyberattaque.

Il ressort de cette analyse la bonne compréhension par le groupe des enjeux de la cybersécurité et de la nécessité de procéder à la mise en place de mesures préventives tant techniques, qu'organisationnelles et juridiques. Les mesures recommandées sont :

D'un point de vue technique :

- Mettre en place la migration de ses données vers une solution d'hébergement auprès d'un cloud service provider (CSP).
- Mettre en place un Plan de Reprise d'Activité (PRA), ensemble de procédures (techniques, organisationnelles, sécurité) qui permettent à l'entreprise de prévoir par anticipation, les mécanismes pour reconstruire et remettre en route un système d'information en cas de sinistre important ou d'incident critique.

Sur le plan organisationnel :

- Création d'un comité de cybersécurité composé du DSI, du DPO, du responsable du support et des outils collaboratifs ainsi que du responsable de l'administration de l'hébergement du CS.
- Mise en place d'un Security Operations Center (SOC), soit l'équipe en charge d'assurer la sécurité de l'information via une plateforme permettant la supervision et l'administration de la sécurité du système d'information au travers d'outils de collecte, de corrélation d'événements et d'intervention à distance. Le SIEM (Security Information Event Management) est l'outil principal du SOC puisqu'il permet de gérer les évènements d'un SI.

Sur le plan juridique :
Nécessité de disposer d'un plan de gestion de crise en cas de cyberattaque afin de minimiser les coûts que pourrait engendrer cette dernière, plan qui mêle à la fois des mesures techniques, organisationnelles et juridiques.

L'élaboration de ce plan s'est effectuée en plusieurs étapes :

- Documentation rigoureuse à l'aide de sources fiables (ANSSI et CLUSIF) pour définir le cadre du plan de gestion de crise en s'accordant sur les termes employés, notamment par le biais d'illustrations.

- Classification des applications vitales pour l'entreprise et leur dépendance en termes de flux. Construction du schéma d'architecture.

- Définition de la cellule de crise (SOC) : son rôle, ses missions et sa composition (membres permanents et mobilisables) avec une typologie des contextes relatifs aux crises pouvant survenir, c'est-à-dire les évènements déclencheurs.

- Préciser les contextes relatifs aux crises pouvant survenir, les « évènements déclencheurs » :
  - Identification de grandes catégories (acte criminel type sabotage, défaillance ou destruction, ...)
  - Identification de situations associées (défiguration de site web, cryptolocking, interruption d'un service tiers, ...)
  - Identification des mesures de détection (monitoring, support, veille, ...)
  - Identification de la première réponse (mitigation, isolation d'actifs, collecte d'information, inventaire, ...)
  - Identification des critères de crise (étendue du périmètre impacté, situation qui perdure, déclenchement immédiat, ...)
  - Identification du pilote de crise
  - Planification de simulation de crise
  - Plan d'action opérationnel et technique
  - Plan de sauvegarde

- Définition des plans d'actions, variables en fonction de ces mêmes événements déclencheurs, prenant en compte l'enjeu que représente la nécessité de communiquer avec la direction pour chaque prise de décision.

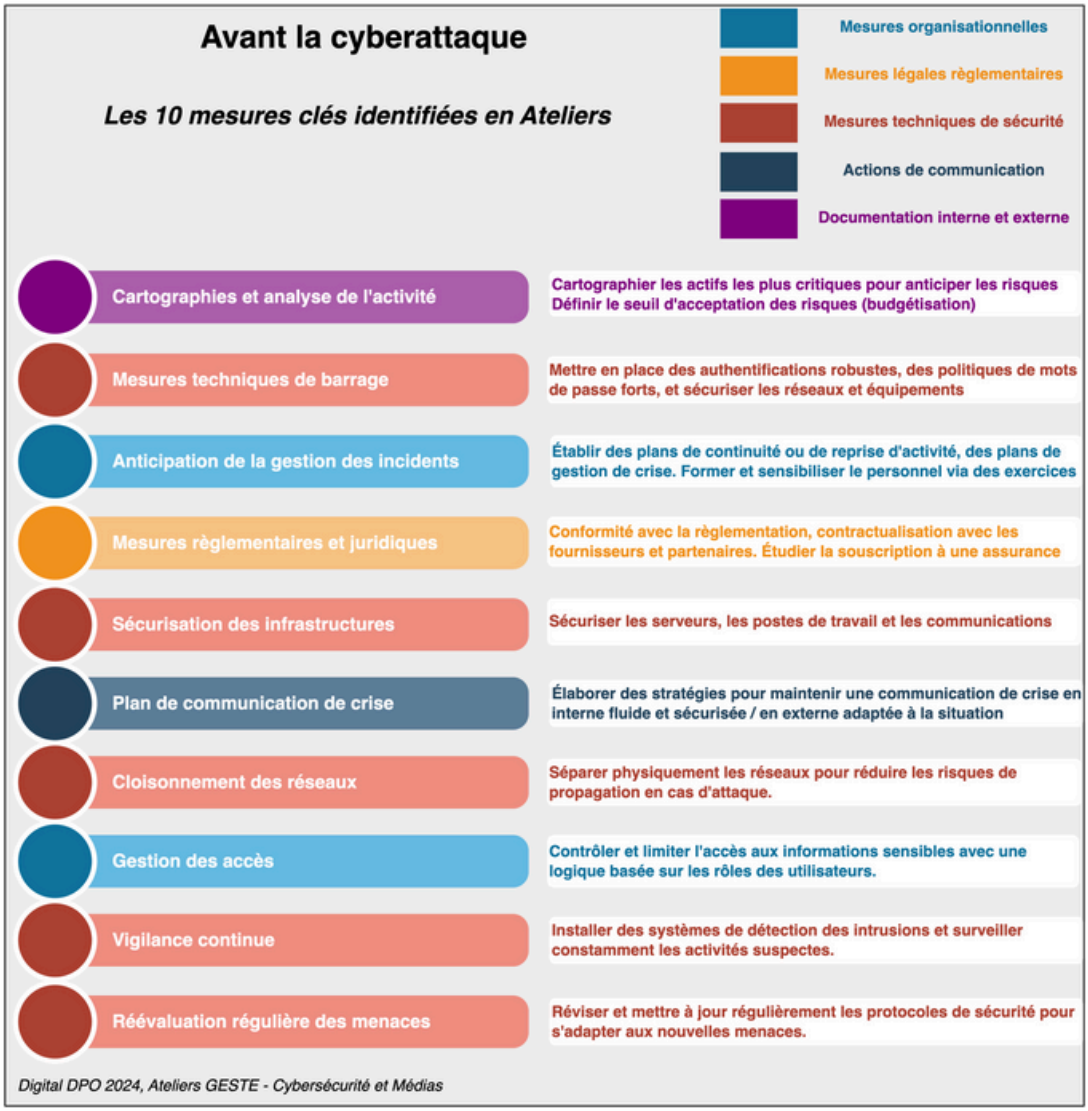
  - Plan de crise « risque sécurité » (renforcement des mesures de protection)
  - Plan de crise « intrusion » (blocage de l'attaquant, remédiation, prévention)
  - Plan de crise « sinistre » (analyse, rétablissement, retour en situation nominale)

- Prévoir un premier niveau de réponses et mesures à prendre et identifier le responsable de chaque action.

Souci majeur identifié : nécessité d'anticiper la perte d'accès aux applications et ressources du groupe de médias, ce qui signifie développer un moyen de préserver les listes de contacts clés (ou activités clés) tels que les clients ou interlocuteurs stratégiques, fournisseurs, etc. dans un objectif de continuité dans la communication, ainsi que les sources.

PARTIE II - LES MESURES DE GESTION DE CRISE CONCOMITANTES À L'ATTAQUE

Dans l'éventualité où le média serait victime d'une cyberattaque, il est nécessaire que la structure soit déjà prête à y faire face et que les organes de direction n'aient qu'à déclencher une série de mesures organisationnelles, techniques (1) et juridiques (2) déjà anticipées permettant de contrôler l'impact de l'attaque. Étudier les protocoles mis en œuvre dans l'urgence par une structure non-équipée permet de souligner ce constat (3).



1 DÉCLENCHER LE PROTOCOLE DE GESTION DE CRISE EN INTERNE : MESURES ORGANISATIONNELLES ET TECHNIQUES

Dans la détermination **des mesures techniques essentielles** pour faire face à une cyberattaque se trouve avant tout le protocole d'identification de la cyberattaque par le biais des données dont dispose la structure en l'état. Cerner au mieux le type de cyberattaque subie permettra en effet aux organes de direction d'orienter avec un maximum de précision la défense du média pour n'avoir à déplorer qu'un minimum de dégâts.

Cela passe évidemment en amont par la détection de la cyberattaque en tant que telle, sa journalisation puis sa corrélation avec un événement interne ou extérieur (trouver la source de la cyberattaque).

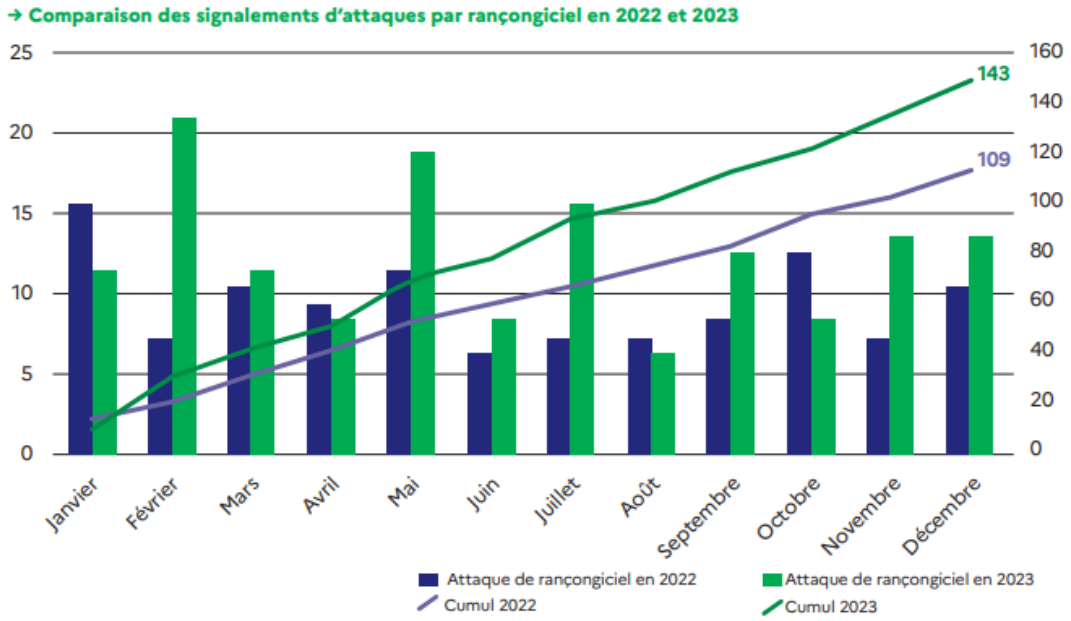
La gestion de l'attaque en tant que telle nécessite d'en mesurer son impact en analysant sa sévérité. Cela permettra par la suite de déclencher les mesures adéquates. **Plus précisément, dans les mesures techniques à mettre en place, la création et la préservation d'une ligne téléphonique ou tous moyens de communication alternatifs permettant de maintenir la communication en interne (notamment pour le process de prise de décision) est une mesure à envisager prioritairement.** A ce titre, **le partage d'un protocole écrit avec coordonnées et numéro de téléphone portable de chaque personne faisant partie de la cellule de crise est une bonne option.**

Sur le plan des mesures organisationnelles à mettre immédiatement en place en cas de cyberattaque, la principale mesure réside dans le déclenchement de la procédure d'alerte et de gestion de crise. Cela implique donc d'activer la cellule de crise mise en place dans le cadre des mesures préventives, de communiquer en interne et éventuellement en externe si besoin s'en fait sentir sur l'exposition du média à une cyberattaque, et de mettre en œuvre le plan de continuité d'activité (PCA). Dans le cas où le plan de continuité d'activité n'aurait pas permis de maintenir le média à 100% de son activité, il sera nécessaire de déclencher un plan de reprise d'activité (PRA) élaboré au préalable, qui permettra de passer au-delà des dégâts occasionnés par la cyberattaque. En cas de coupure prolongée des services, il est impératif pour un média de basculer rapidement sur un mode de publication dégradé. Cette approche permet de maintenir la diffusion des informations essentielles tout en limitant l'impact sur l'audience et les partenaires. Les plans de publication en mode dégradé doivent être prêts à être activés immédiatement pour assurer une continuité minimale des services.

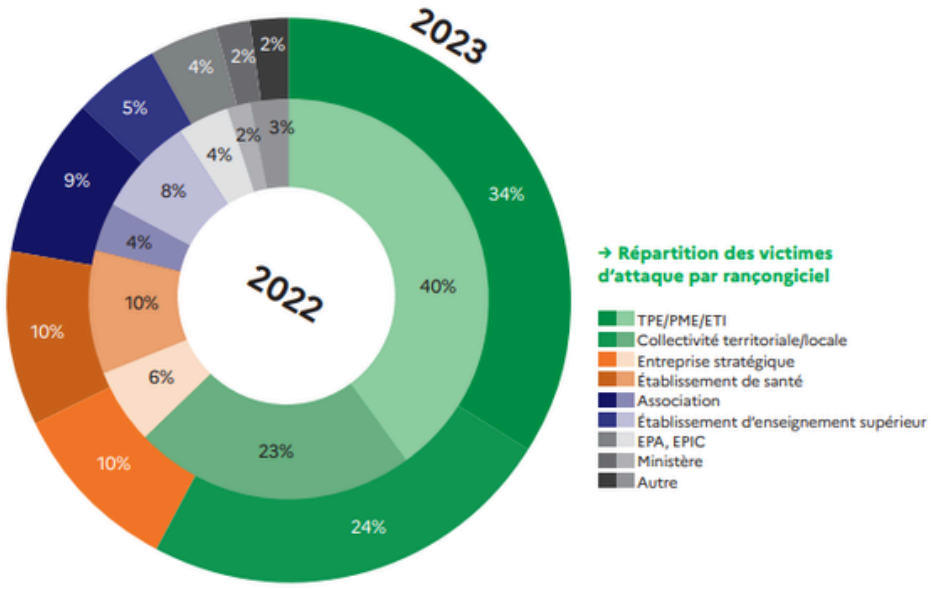
Focus sur la cyberattaque par rançonnage

[21] ISO 22301 : 2012 Systèmes de management de la continuité d'activité - www.iso.org - Guide pour réaliser un plan de continuité d'activité, SGDSN, 2015 - www.sgdsn.gouv.fr/uploads/2016/10/ guide-pca-sgdsn-110613-normal.pdf - Plan de continuité d'activité à l'usage du chef d'entreprise en cas de crise majeure, DGE, 2015 - www.entreprises.gouv.fr/files/files/directions_services/politique-etenjeux/entrepreneuriat/Guide-PCA-en-cas-de-crisemajeure.pdf

Dans son panorama de la cybermenace publié en 2023, l'ANSSI établit un constat inquiétant sur l'augmentation et la pérennisation de la pratique du rançonnage, plus particulièrement par utilisation d'un rançongiciel.[22]



L'ANSSI parvient également à répartir les victimes d'attaque par rançongiciel par types de structures touchées : les très petites et moyennes entreprises ainsi que les entreprises de taille intermédiaire (dans lesquelles la plupart des médias peuvent entrer) sont les plus visées. L'ANSSI relève également par le graphique ci-dessous l'augmentation des attaques par rançongiciel affectant les associations, forme sous laquelle les médias sont également susceptibles d'exercer leur activité.



[22] « Lors d'une attaque par rançongiciel, le cybercriminel met l'ordinateur ou le système d'information de la victime hors d'état de fonctionner de manière annoncée réversible. Les utilisateurs perdent ainsi le contrôle de toutes les informations stockées sur l'appareil. L'attaquant adresse alors généralement un message à la victime en lui proposant de lui fournir le moyen de déchiffrer ses données contre le paiement d'une rançon. Les pirates informatiques demandent des rançons à la victime en échange de l'accès rendu aux données corrompues, et dans certains cas de plus en plus fréquents pour accentuer la pression sur la victime, ils menacent de rendre public les données dérobées » - définition proposée par cybermalveillance.gouv.fr dans un article publié le 2 mars 2022.

En présence d'une attaque par rançongiciel, la toute première des réponses et dont il faut parvenir à ne pas se défaire malgré parfois une forte tentation, est le refus de payer : **par principe, il ne faut en effet jamais payer**. Rien ne garantit en effet que le média atteint retrouvera ses données en clair en cas de paiement en plus de participer au financement des activités illégales (cybercriminalité).

2 AMORCER LES MESURES JURIDIQUES IMPLIQUANT DES PARTIES PRENANTES EXTÉRIEURES

Dès qu'une cyberattaque se déclare au sein du média, les organes de direction doivent envisager les mesures juridiques qu'impliquent les dommages qui en découleront.

- Si des données personnelles sont potentiellement touchées par la Cyberattaque, notification de la faille auprès de la CNIL en ligne : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles dans le délai de 72 heures. À savoir : avant de remplir votre notification en ligne, vous pouvez utiliser ce document préparatoire qui reprend les étapes de la marche officielle. Ce téléservice est uniquement dédié aux responsables de traitement (organismes privés ou publics) souhaitant notifier à la Commission une violation ayant touché les données personnelles qu'ils traitent. Cette notification initiale pourra toujours être complétée ensuite en fonction des éléments recueillis.

- Prise de contact avec l'ANSSI voire obligation de déclaration de l'incident et/ou CERT-FR qui peut apporter une assistance précieuse.

- Dépôt d'une plainte auprès des autorités compétentes dans les 72 heures suivant la prise de connaissance de la cyberattaque. Ce dépôt de plainte est en effet, depuis la Loi de Programmation du ministère de l'Intérieur du 24 janvier 2023, une obligation à laquelle il est nécessaire de se soumettre pour que la cyberattaque soit prise en compte par l'assureur couvrant les cyber risques du média.

L'obligation de déposer une pré-plainte dans les 72 heures ouvre toujours la possibilité néanmoins de compléter les faits recensés au fil de l'eau.

Il ne faut pas oublier de procéder à une délégation de signature pour le dépôt de plainte et de manière générale de prévoir une procédure particulière de délégation de dépôt de plainte pour les périodes sensibles (vacances et week-end).

- Activation de la couverture prévue par le contrat d'assurances conclu le cas échéant dans le cadre des mesures préventives (voir supra), ce qui implique dans un premier temps de faire la déclaration de sinistre, sur la base de la plainte réalisée auprès des autorités. La simple exposition au risque peut également être couverte, en fonction de l'étendue de la couverture prévue.

Les coûts pris en compte sont de manière générale les procédures de remédiation mises en œuvre, la sécurisation du système d'information et éventuellement la rançon payée.

Cette dernière ne pourra toutefois être remboursée que si elle n'a pas été expressément exclue du champ d'application de l'assurance et si une plainte a été déposée dans les 72 heures suivant la connaissance, par le média, de la cyberattaque.

ATTENTION : il existe plusieurs situations dans lesquelles l'assureur sera susceptible de refuser de couvrir le sinistre subi par le média du fait d'une cyberattaque : lorsque le(s) cyberattaquant(s) font en réalité partie d'un groupe adossé à un État, ce qui n'est pas improbable dans le cas d'une tentative de déstabilisation d'un média français par une autorité étrangère, la prise en compte du dommage par l'assureur pourra être refusée.

CONSEILS : se faire accompagner par son avocat rompu à la gestion de crise, notamment dans le domaine des cyberattaques, pour encadrer les différentes actions qu'il convient de mener de front en un minimum de temps.

3 APPROFONDIR SON APPROCHE PAR L'ANALYSE DE LA RÉACTION CONCRÈTE D'UN MÉDIA FACE À UNE CYBERATTAQUE

TV5 Monde, grand groupe de médias international francophone, a été victime d'une attaque ciblée contre ses réseaux informatiques. Ce groupe a accepté de partager avec le GESTE son expérience de la gestion de cette situation, permettant ainsi de présenter dans ce Livre Blanc un cas concret de réaction immédiate à ce type de situation en l'absence de prévention en amont.

Le groupe a ainsi fait l'objet d'une attaque ciblée au cours d'une période de 90 jours pendant laquelle les attaquants ont réussi notamment à collecter une importante quantité d'informations leur permettant de cartographier précisément le système d'information du groupe. En ciblant spécifiquement un administrateur et un prestataire du groupe (via une attaque en ingénierie sociale, en l'espèce un hameçonnage encore dit phishing) les cyberattaquants sont ainsi parvenus à établir des canaux de communication avec leurs propres infrastructures, à récupérer des secrets d'authentification et à monter en privilèges sur les services les plus critiques (réseaux et systèmes). En combinant cet ensemble de moyens, les attaquants ont pu lancer leur attaque et détruire méthodiquement de façon coordonnée et rapidement une partie des actifs essentiels (service de messagerie, serveurs de diffusion, etc.) et défacer les plateformes web (sites Internet, réseaux sociaux) du groupe.

Immédiatement à la suite de la détection de l'incident, et en l'absence d'indices suggérant une panne (les services étaient alors stoppés les uns après les autres), le groupe de médias a pris la lourde décision, mais finalement salvatrice, de couper de toute urgence tout accès à internet, puis de prévenir les autorités et de réunir sa cellule de crise composée de quelques membres clés du comité directeur et de la direction technique.

Le matériel compromis alors isolé, l'ANSSI a pu accompagner durant plusieurs semaines les équipes techniques du groupe dans l'analyse du chemin d'attaque et dans la définition et la mise en place des mesures de remédiation et de reconstruction de ses systèmes.

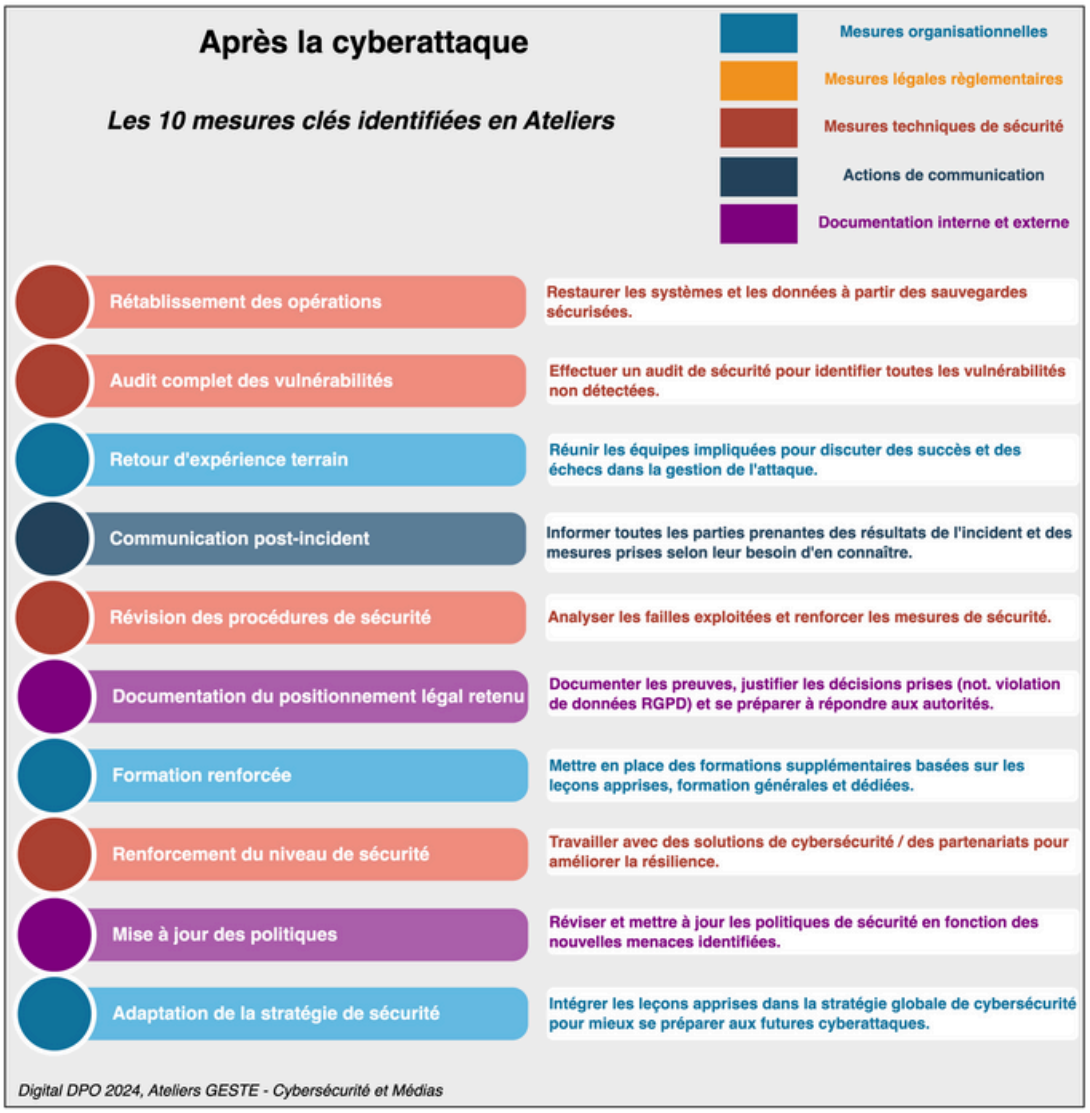
L'objectif de cette attaque était de détruire la chaîne - constat corroboré par l'absence de demande de rançon — et de porter atteinte à l'image de la France de manière générale déstabilisant l'un de ses piliers, la presse, matérialisée ici par l'activité d'un de ses plus grands groupes de médias.

Les coûts en termes financiers et humains ont été très élevés. Ces coûts supplémentaires ont été estimés à 4,4 M€ la première année, à 3,7 M€ la deuxième année puis à environ 3 M€ de coûts récurrents dès les années suivantes (environ 15% du budget de la direction des systèmes d'information du groupe)[23]. La mobilisation de certaines catégories du personnel de jour comme de nuit avec la violence psychologique et le stress inhérents à toute crise, le recours à des prestataires extérieurs pour procéder aux mesures de remédiation et reprendre la diffusion de la chaîne de télévision dès que possible ainsi que le chiffrage du montant total de la note ont permis de constater qu'il était plus bénéfique d'investir proactivement dans la prévention.

[23] Source: https://www.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2017/pap/html/DBGPGMOBJINDPGM847.htm

PARTIE III - LES MESURES CONSÉCUTIVES À L'ATTAQUE

La période suivant la cyberattaque est déterminante pour l'avenir : il s'agira de gérer les conséquences directes de l'attaque sur son environnement en communiquant à son sujet (1) mais également d'analyser en profondeur les loupés et les réussites de la gestion de crise de la cyberattaque en anticipant celles qui pourraient survenir dans des temps futurs (2). Se pencher sur un cas concret de gestion post-attaque permettra d'illustrer le propos (3).



1 ÉLABORER UN PROTOCOLE DE COMMUNICATION AU PUBLIC SUR LA CYBERATTAQUE

D'un point de vue organisationnel, il est nécessaire pour le média ayant subi une cyberattaque de préparer sa communication en externe.

Quelques conseils doivent être suivis.

- Au niveau temporel : il n'est pas nécessaire d'attendre l'arrêt total de la cyberattaque et de la gestion de la crise pour commencer à lancer sa communication sur le sujet : dès lors que l'information est partagée à l'extérieur du média (prestataire extérieur d'assistance cybersécurité, ANSSI, CNIL…) elle circulera ; il faut donc que les organes de direction du média prennent les devants et communiquent d'eux-mêmes sur la situation. Ne pas omettre non plus l'éventuelle obligation de communiquer auprès des personnes dont les données personnelles ont été compromises ou volées, qui peut engendrer des milliers d'emails d'information à envoyer. La coordination entre les divers niveaux de communication est donc primordiale.

- Au niveau du contenu des éléments communiqués : il faut chercher à maintenir un certain niveau de transparence tout en protégeant la structure, en s'assurant de ne pas dévoiler des vulnérabilités encore non résolues ou de ne pas ternir l'image du média. Cela étant dit, il est possible de définir une liste non-exhaustive de sujets à aborder dans la communication extérieure : divulguer des informations sur le type d'attaque subie et les mesures prises en amont et lors de l'attaque peut déjà être une première manière de rassurer les acteurs de son environnement économique (fournisseurs, clients, public…) sur la maîtrise de la situation. Il peut également être bienvenu d'assumer directement sa part de responsabilité dans l'attaque mais surtout de relever que le média saura répondre des conséquences de la cyberattaque pour les acteurs environnants à l'encontre desquels l'attaque a été préjudiciable. Enfin, il est nécessaire de rendre compte de la situation à date et de souligner qu'il sera fait un retour d'expérience dès la régularisation de la situation.

- Au niveau de la tournure générale de la communication : donner à ses propos une tonalité à la fois rassurante à l'égard de ses partenaires mais également plus offensive que défensive peut être bénéfique pour l'image du média quant aux risques cyber auxquels il fait face : affirmer avoir pris des mesures directement à l'encontre des cyberattaquants peut donner une image positive du média quant à la maturité de sa politique de cybersécurité.

Point d'importance : si la communication est réalisée en interne, il est primordial de déterminer un protocole de validation par les organes de direction des messages, communiqués et contenus mis à disposition du public sur le sujet de manière générale, notamment afin d'assurer leur cohérence et leur conformité au regard du degré de transparence décidé. Néanmoins, il peut être pertinent de faire appel à des communicants spécialisés dans le traitement de sujets aussi délicats pour préparer des éléments de langage et aider chacun à répondre aux éventuelles questions des journalistes d'autres médias qui couvriront l'événement.

Parmi les mesures juridiques à envisager, il faut enfin anticiper toute potentielle enquête de l'ANSSI sur les mesures mises en œuvre en amont et en aval de la cyberattaque. Une enquête pourrait également être menée sur le fondement du respect de la réglementation sur les données personnelles par la CNIL[23] si la cyberattaque a occasionné la mise en cause de données personnelles (compromission de l'intégrité, de la confidentialité…). Par ailleurs, la responsabilité civile ou pénale des dirigeants pourrait être soulevée par les éventuelles victimes collatérales de cette cyberattaque.

2 TRAVAILLER SUR LES RETOURS D'EXPÉRIENCE CONSÉCUTIFS À L'ATTAQUE

Mettre en place de manière systématique un retour d'expérience à la suite de l'exposition du média à une cyberattaque doit être un des nombreux réflexes des organes de direction.

Ce retour d'expérience implique de faire un bilan complet après l'incident.

- En amont tout d'abord, quelles mesures techniques, organisationnelles et juridiques préventives ont permis d'assurer la minimisation des dégâts ? Quelles mesures au contraire doivent être renforcées ? Sur la gestion même de la crise, il faut tenir le même raisonnement et chercher notamment à identifier les personnes qui y contribuent positivement et celles qu'il conviendra d'écarter à l'avenir dans les protocoles de gestion de cyberattaque.
- Par ailleurs, d'un point de vue technique et commercial, il est nécessaire (i) de prévoir les conséquences pratiques des éventuels retours massifs et houleux des clients, fournisseurs etc. sur l'incident, ce qui implique notamment de mettre en place une gestion des appels entrants efficace et (ii) de préparer un courrier type mais également personnalisé en fonction du profil du cocontractant pour minimiser la mise en cause de sa responsabilité. Un soin particulier doit être apporté à la rédaction d'un tel courrier dont l'impact peut être soit rassurant soit délétère si maladroit.
- Une fois l'attaque contenue, il est crucial de revoir les stratégies de publication en mode dégradé qui ont été mises en œuvre. L'analyse de leur efficacité permettra de les améliorer et de s'assurer que, lors de futures crises, le média pourra continuer à informer le public même dans des conditions difficiles. Les retours d'expérience doivent donc inclure une évaluation de ces mécanismes.

Par ailleurs, après analyse du bilan d'incident, il faudra mettre en place une veille sur les outils technologiques permettant d'améliorer de manière continue le niveau de cybersécurité du média pour minimiser les risques qu'une telle cyberattaque se reproduise.

De même, il conviendra de chercher à améliorer les protocoles de sécurité en fonction de l'expérience retirée de la gestion de la crise, toujours en adéquation avec le plan d'amélioration continue de la sécurité (PACS) évoqué lors de nos développements sur les mesures préventives.

Enfin, si la cyberattaque a lieu en l'absence de toute mesure préventive, il conviendra de pallier cette carence en mettant en place les mesures qui ont fait cruellement défaut lors de la gestion de crise.

3 ENRICHIR SON SAVOIR PAR L'ANALYSE DE MESURES POST-ATTAQUES RÉELLES

Le grand groupe de médias français dont il était question lors de l'analyse d'une gestion concrète d'une cyberattaque a également accepté de partager les mesures techniques et organisationnelles mises en place à la suite de l'attaque ciblée dont il a été victime (voir supra I. 3.).

Les actions mises en œuvre post-crise reprennent notamment des mesures qui auraient dû être mises en place préventivement au sein de la structure mais qui, à date de l'incident, ne faisaient l'objet que de peu d'informations à l'époque dans le secteur en l'absence totale de prise de conscience.

Ainsi, des formations ont été organisées permettant de sensibiliser à ces enjeux cybersécurité l'ensemble des personnes œuvrant au sein de la structure avec une communication spécifique auprès des collaborateurs sur la manière de gérer et de former les nouveaux arrivants sur cette problématique.

La structure a également consacré un budget important à la cybersécurité (matériels, recrutement...).

Les organes de direction se sont par ailleurs accordés sur la nécessité d'intégrer un volet « sécurité » à chaque projet, mettant notamment en place un clausier de sécurité à intégrer de manière systématique à tous les contrats, un process de validation de l'architecture technique d'un projet auprès du service sécurité, etc.

Enfin, il s'est avéré nécessaire de s'assurer de la compliance des éditeurs et des prestataires externes à leurs obligations de cybersécurité : les certifications ISO 27001 n'étant pas les uniques critères, le groupe a décidé de mettre en place un questionnaire permettant de s'assurer de la fiabilité de ces acteurs en termes de maîtrise des risques cyber avant d'engager ou de poursuivre une relation avec ces derniers.

CONCLUSION : La cybersécurité est l'affaire de tous !

ANNEXE 1 : AUTRES GUIDES OU LIVRES BLANCS SUR LA CYBERSÉCURITÉ

https://www.ifa-asso.com/mediatheques/guide-securite-numerique-et-gouvernance/

https://bigmedia.bpifrance.fr/etudes/cybersecurite-un-guide-pratique-a-destination-des-dirigeants?pk_vid=59d0ef1776d473b01713448443a6bfe4

https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/

ANNEXE 2 : RACI DE RÉPARTITION DES MESURES ENTRE LES PARTIES PRENANTES

Définition des rôles et responsabilités des acteurs

- **DPO** (Data Protection Officer)

Rôle : Assurer la conformité de l'entreprise avec le RGPD et autres réglementations relatives à la protection des données.

Responsabilités :
- Surveiller et évaluer les risques liés à la protection des données personnelles.
- Collaborer avec la DSI sur l'évaluation des risques et la mise en place des mesures.
- Assurer la formation et la sensibilisation du personnel aux obligations de protection des données.
- Gérer la notification et la communication autour des violations de données.

- **DJ** (Direction Juridique composée du juriste et/ou de l'avocat) et personnes en charge des assurances cyber.

Rôle : Anticiper les points de responsabilités contractuelles avec les tiers. Évaluer les implications juridiques des incidents et conseiller sur la posture à prendre vis-à-vis des tiers.

Responsabilités :
- Collaborer étroitement avec le DPO pour s'assurer que toutes les actions prises lors des phases avant, pendant et après une cyberattaque sont légalement conformes.
- Documenter l'incident, coordonner les actions nécessaires auprès des autorités compétentes et des assureurs.
- Participer à la rédaction et la révision des politiques de sécurité et de confidentialité.
- Conseiller la cellule de crise sur les aspects légaux durant les incidents de sécurité, notamment les responsabilités des tiers ou vis-à-vis des tiers.
- Assister les équipes dans la gestion des litiges ou des actions en justice résultant de cyberattaques ou de violations de données.

- **RSSI** (Responsable de la Sécurité des Systèmes d'Information) ou à défaut DSI, CIO ou responsable identifié de la cybersécurité

Rôle : Développer, mettre en œuvre et surveiller la stratégie de sécurité de l'entreprise pour protéger les ressources informatiques.

Responsabilités :

- Gérer la sécurité des systèmes d'information, incluant la prévention des risques, la détection des menaces et la réponse aux incidents.
- Conduire des audits de sécurité et des évaluations des risques réguliers.
- Superviser la cartographie des actifs critiques et la gestion des accès aux systèmes.

- **Équipe IT**

Rôle : Maintenir et sécuriser les infrastructures informatiques de l'entreprise.

Responsabilités :

- Installer, configurer et mettre à jour les systèmes de sécurité informatique.
- Assister dans la gestion des accès et maintenir la sécurité des données et des applications.
- Participer aux interventions techniques lors des incidents de sécurité.

- **Prestataires externes** (sécurité informatique, consultants)

Rôle : Fournir une expertise et un soutien spécialisés en matière de sécurité informatique.

Responsabilités :

- Conseiller l'entreprise sur les meilleures pratiques de sécurité et les technologies adaptées.
- Participer à la mise en œuvre de projets de sécurité spécifiques.
- Offrir des services de formation et de sensibilisation pour le personnel.

- **Cellule de crise**

Rôle : Coordonner et gérer la réponse à un incident de sécurité majeur.

Responsabilités :

- Activer les procédures d'urgence et coordonner les actions entre les différents acteurs impliqués.
- Communiquer efficacement tant à l'intérieur qu'à l'extérieur de l'organisation.
- Documenter l'incident et les réponses pour l'analyse post-incident.

- **Équipe de communication**

Rôle : Gérer toutes les communications externes et internes lors d'un incident de sécurité.

Responsabilités :

- Préparer et diffuser les informations sur l'incident aux médias et autres parties prenantes externes.
- Assurer la communication interne pour maintenir la confiance et l'ordre au sein de l'organisation.
- Surveiller la couverture médiatique et les réactions du public.

Support complémentaire : composition type de la cellule de crise

- Directeur de la sécurité de l'information (RSSI)
- Responsable des systèmes d'information (ou directeur informatique)
- DPO (Data Protection Officer)
- Responsable des communications
- Représentant de la direction (parfois le Directeur Général ou un membre du conseil d'administration)
- Experts techniques selon l'incident (membres de l'équipe IT ou prestataires externes)
- Conseiller juridique et/ou avocats (pour les implications légales des incidents)

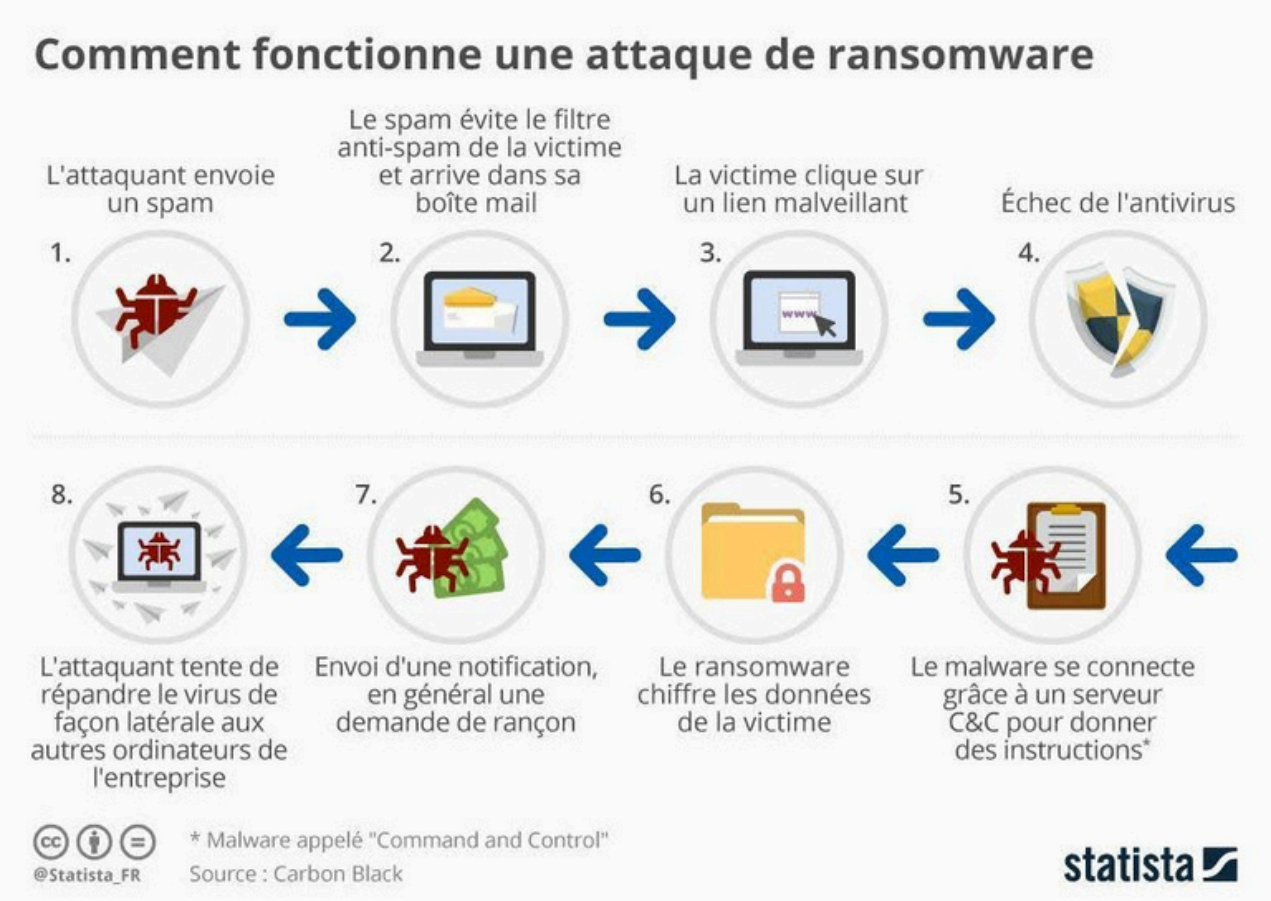
Le tableau ci-après présente une vision discutée dans le cadre de l'Atelier des interactions entre l'ensemble des acteurs au cours des 3 phases identifiées dans le Livre Blanc.

Dans ce type de matrice, il est à noter qu'il ne peut y avoir qu'un seul « R » positionné en responsabilité de la réalisation effective de chaque action. NB : Plusieurs abréviations sont utilisées dans le tableau de responsabilités ci-dessus : R : Responsable, A : Approuve, C : Consulté, I : Informé

#	Actions	DPO	DJ	RSSI	Équipe IT	Experts externes	Cellule de crise	Direction	Communication
AVANT	Cartographie des actifs critiques	I	I	R	A	C	I	I	
	Évaluation des risques	A	C	R	C	C		A	
	Allocation de ressources pour la sécurité	C		C	C		I	R	
	Mise en place des mesures préventives techniques	C		R	A	A		A	
	Mise en place des mesures préventives juridiques (conformité)	R	C	C				A	
	Mise en place des mesures préventives juridiques (assurances)	C	R	C				A	
	Gestion des accès aux systèmes	C		R	A	A			
	Formation et sensibilisation	A		R	C	A			
	Planification de la reprise après sinistre	I	I	C	C	I	I	R	I
PENDANT	Gestion de la crise (mesures en réaction)	I	C	A	A	I	R		C
	Identification et confinement des impacts	I	C	C	R	C	A		I
	Notification des violations de données	R	C	A	C	I	C	I	A
	Communication interne/externe	I	C	C	I	I	A	A	R
APRÈS	Audit de sécurité et ajustement des mesures	I	C	R	A	C	C	I	I
	Audit légal et communication avec la CNIL	R	C				I	A	
	Communication post-incident	I	C	I	I	I	I	C	R
	Documentation interne	A	A	A	A	I	R		I
	Mise à jour des politiques et des protocoles	A	C	R	A	C	C		I
	Amélioration continue des processus	A	A	R	A	C	C	A	I
	Évaluation des impacts financiers et opérationnels	C	C	A	A		R	I	
	Renforcement des partenariats stratégiques	C	C	C	C	A		R	

Digital DPO 2024, Ateliers GESTE - Cybersécurité et Médias

ANNEXE 3 : SCHÉMA D'UNE ATTAQUE PAR RANSOMWARE



TÉMOIGNAGES

"La cybersécurité est une préoccupation constante des équipes techniques depuis plusieurs années. Nous travaillons à unifier les procédures de cybersécurité dans l'ensemble du groupe, les renforcer, et à faire grandir la culture cyber auprès de tous les salariés. La donnée est notre bien le plus précieux, nous la protégeons."

bayard

"Vos données sont précieuses, sauvegardez-les régulièrement. Face aux ransomwares, les sauvegardes restent le dernier rempart.
La sensibilisation des collaborateurs aux risques cyber améliore la sécurité de l'entreprise.
Les correctifs de sécurité : une défense essentielle contre les vulnérabilités. Un logiciel à jour, c'est une faille en moins."
James BONNAVENTURE, Groupe Le Figaro

"Avant toute collaboration avec un sous-traitant, nos équipes s'efforcent d'évaluer les mesures de sécurité mises en place par ce sous-traitant afin de protéger les données personnelles en jeu. Nous avons ainsi formalisé une procédure nous permettant, en amont de la négociation du contrat et en étroite collaboration avec nos services DSI et RSSI, de recenser l'ensemble des mesures de sécurité et d'en analyser la qualité et la pertinence." **Anne GUILBERT, Responsable juridique**

CMI FRANCE

TV5 MONDE

"Connaitre et maitriser ses risques permet d'identifier les scénarios de crise contre lesquels nous devons nous préparer en priorité."
"Ne pas hésiter à débuter modestement la construction de son plan de gestion crise puis à réitérer régulièrement afin d'enrichir de son expérience les différents scénarios de crise et plans de réponse." ***Yoann PAOLONI, Responsable Sécurité des SI***

“Au sein du Groupe TF1, nous mettons tout en œuvre pour anticiper et se prémunir des attaques cyber en formant et sensibilisant nos collaborateurs sur les risques Cyber et en mettant en œuvre des moyens importants de protection, de détection et réaction aux événements de sécurité. Nous réalisons aussi des exercices de crise avec des scénarii plausibles pour nous entraîner” / “La préparation est la clé pour faire face aux attaques cyber.”

“Pour Radio France, ainsi que pour les sociétés dans le domaine de l’audiovisuel, la continuité d’activité se concentre en premier lieu sur les processus critiques de diffusion.
En cas de compromission du système d’information, les équipes se mobilisent sur la continuité d’activité sur un système complètement dissocié du système nominal, idéalement depuis un site de secours pour éliminer toute adhérence physique et logique.
Première ligne de redémarrage après sinistre, les sauvegardes font l’objet d’une attention particulière, car tout comme les données de production, elles sont également les cibles privilégiées d’un cyberattaquant pour contraindre la victime à payer une rançon.
Dans une telle situation, il faut avoir la certitude de restaurer des sauvegardes saines, autrement dit non compromises par l’attaquant. Pour protéger ces actifs support précieux, il est nécessaire de les préserver en séquestrant des sauvegardes hors ligne ; d’avoir confiance dans la capacité à restaurer des sauvegardes en les relisant, mieux en réalisant des tests de restauration périodiquement ; de s’assurer de leur intégrité en réalisant une remontée en temps réel des alertes associées à un éventuel démarrage de leur chiffrement et en ayant la possibilité de les inspecter en recherchant des marqueurs de compromission.
Un plan ordonnancé pour la reconstruction des services du système d’information complète ce dispositif.”

“Les avocats en cybersécurité sont aux côtés de leurs clients avant, pendant et après une cybercrise. Par expérience, la complémentarité des compétences techniques, organisationnelles et juridiques est essentielle, sans compter celle moins connue des « soft skills » représentés au sein des équipes qui seront sur le pont.

Plus tôt nous intervenons à la demande des clients, plus notre intervention est gage de plus-value pour eux, notamment en encadrant au mieux leur risque réputationnel interne et externe.”

Corinne THIÉRACHE
Alerion Avocats

“En tant que DPO, j’ai fait face à des cyberattaques majeures qui ont entravé les activités de médias pendant plusieurs semaines. Ces crises ont démontré que la cybersécurité doit être une priorité stratégique, abordée avec méthode en amont, discernement pendant l’action, et sérénité en aval. Les erreurs et les leçons apprises m’ont convaincu qu’une approche holistique, intégrant les dimensions techniques, organisationnelles, juridiques et humaines, est indispensable.

Cette idée irrigue ce livre blanc qui n’est pas seulement un guide ; c’est un appel à l’action pour les dirigeants. Leur implication active, combinée à l’expertise des RSSI et DPO, soutenue par une stratégie de résilience et d’amélioration continue, est essentielle pour garantir la sécurité opérationnelle des actifs, assurer la diffusion des contenus et protéger les médias.”

Sébastien GANTOU
Digital DPO

GESTE

CONTACT

GESTE
76 Rue de Richelieu
75002 PARIS

https://geste.fr/