L’établissement d’un plan de réponse en cas de faille de sécurité

Philippe Gilliéron, le 17 mai 2021

L’établissement d’un plan de réponse en cas de faille de sécurité constitue une étape essentielle lors de la mise sur pied d’un plan de gestion en matière de données au sein des entreprises. Cette contribution s’efforce d’en retracer de manière synthétique les différentes étapes et leur contenu.

I. Introduction

« *As described above, having regard to the impact of the Covid-19 pandemic (On Marriott and more generally), and consistently with the Commissioner’s published guidance, [T]he final penalty payable will therefore be reduced to £18.4 million* ». Tels sont les termes dont le conseil d’administration du groupe Mariott a pris connaissance le 30 octobre dernier en tournant sans doute avec anxiété les pages de la décision rendue par l’ICO, après avoir subi un incident en matière de sécurité ayant exposé environ 339 millions de fichiers de clients. CÉLIAN HIRSCH s’en faisait récemment l’écho ici même.

Ce cas est loin d’être isolé, preuve en est le rapport publié en fin d’année dernière par *Risk Based Security* faisant état de 2’935 incidents ayant mené à la divulgation de 36 milliards de fichiers durant les seuls neuf premiers mois de l’année 2020.

Aujourd’hui, la question n’est donc pas tant de savoir « si », mais « quand » un tel incident va se produire et avec quelle ampleur. Si les risques sont nombreux, tout aussi nombreux sont les organismes s’efforçant de les identifier pour s’en prémunir. Parmi ces initiatives, mentionnons celles, devenues un standard et récemment utilisées comme référentiel sur le plan contractuel, de la Fondation OWASP, qui référence de manière périodique les dix préoccupations majeures en termes de sécurité.

En toute hypothèse, nonobstant les efforts déployés, éviter ces risques *ad eternam* apparaît peu probable. Fort de ce constat, les détecter et y remédier aussi rapidement que possible apparaît comme une condition *sine qua non* pour éviter d’avoir à passer sous les fourches caudines des autorités.

Ces fourches peuvent s’avérer particulièrement piquantes. En 2020, les sanctions pronon-

cées sur le fondement de l'art. 32 RGPD se sont montées à plus de 83 millions d'euros ; entre 2018 et 2020, les amendes infligées par les autorités de protection des données dans les États de l'Union européenne sur le fondement d'un défaut de sécurité auraient ainsi été multipliées par 162 si l'on en croit un article paru dans le Journal du Net.

Conjugué à l'obligation faite à l'art. 33 RGPD aux responsables de traitement de notifier la violation des données à caractère personnel aux autorités lorsqu'il en résulte un risque pour les individus concernés, une obligation qui existera également en Suisse après l'entrée en vigueur de l'art. 24 nLPD[1], le risque découlant d'un tel incident fait de l'adoption d'un plan de réponse une étape primordiale dans la mise en œuvre d'un plan de gestion digne de ce nom en matière de données.

Cette brève contribution a pour objectif de décrire de manière sommaire les étapes liées à l'établissement et la mise en œuvre d'un tel plan.

II. Établissement d'un plan de réponse en cas de faille de sécurité

Il existe deux grands modèles pour établir un plan de réponse en cas d'incident : celui du *National Institute of Standards and Technology (NIST)* d'une part et celui du *Sysadmin, Audit, Network, and Security (SANS)* d'autre part. Ces modèles comprennent les phases suivantes, que nous allons reprendre l'une après l'autre :

- préparation [a] ;
- détection et analyse [b] ;
- confinement, suppression et récupération [c][2] ;
- enseignements [d].

a) Préparation

Cette première étape consiste en un premier temps à déterminer l'équipe en charge de gérer l'incident puis, en un second, d'apprécier les ressources dont dispose l'entreprise pour gérer l'incident.

La structure donnée à l'équipe en charge de répondre à l'incident sera propre à la structure de l'entreprise. Centralisée au travers d'une seule équipe pour les PME, elle sera le plus souvent décentralisée lorsque l'entreprise est présente sur différents marchés ou subdivisées en de nombreuses unités, hypothèse dans laquelle la coordination jouera un rôle important quant à l'efficacité de la réponse donnée à l'incident.

En toute hypothèse, répondre à un incident requiert une coordination entre de nombreux acteurs aux rôles différents au sein d'une entreprise, parmi lesquels : la direction (responsable à la fin de la gestion de l'incident et donc à tenir informée en premier lieu), le support IT (à même de prendre les mesures adéquates rapidement concernant les systèmes concernés), le service juridique (à même d'apprécier les obligations légales résultant de l'incident, notamment quant au devoir de notification), les ressources humaines (si l'incident concerne les employés) ou encore la communication (susceptible d'entrer en jeu lorsqu'il s'agit d'informer les médias de la survenance de l'incident eu égard à sa nature) pour prendre les plus courants. Ces différents acteurs et le rôle qu'ils seront respectivement amenés à jouer dans le cadre de la gestion de l'incident doivent être clairement identifiés.

La deuxième étape consiste à faire un inventaire des ressources à disposition pour être à même de gérer un incident. Ces ressources sont généralement de trois ordres : (i) organisationnel tout d'abord, en s'assurant que tous les membres de l'équipe sont à même de joindre les autres membres (téléphones portables notamment) et la chaîne de *reporting* ; (ii) matériel ensuite, en s'interrogeant sur les appareils et logiciels à disposition pour traiter l'incident (analyse forensique, ordinateurs de réserve, imprimantes portables, disques externes, etc.) ; (iii) en termes d'outils d'analyse disponibles pour mieux appréhender l'incident enfin (listes des ports, documentation, diagrammes des réseaux et liste des biens critiques, etc.).

À l'issue de la préparation, l'équipe mise en place devrait être en mesure de répondre positivement aux questions suivantes :

- chacun connaît-il les politiques en matière de sécurité de la société ?
- chacun sait-il à qui il doit rapporter et avec qui il doit prendre contact en cas d'incident ?
- les personnes en charge de traiter l'incident ont-elles accès aux journaux et outils permettant de mettre en œuvre le processus de réponse mis sur pied ?
- chacun a-t-il pris part à des exercices de mise en œuvre du plan de réponse (*worktable exercise*) ?

Enfin, à partir du moment où la documentation revêt un aspect crucial dans la gestion d'un incident, il est utile de savoir où aller chercher des modèles de documents auxquels il conviendra de recourir ; on en trouvera d'utiles en libre accès mis à disposition par le SANS.

b) Détection et analyse

Pour être en mesure de détecter un incident, il convient de surveiller les différents systèmes

en place. Pour ce faire, plusieurs types d'outils sont disponibles, parmi lesquels :

- *IDS-IPS* : ces deux systèmes sont liés à l'infrastructure réseau. Alors que le système de détection d'intrusion (*intrusion detection system*) ne fait que collecter des informations[3], le système de prévention (*intrusion prevention system*) permet d'opérer un tri dans les paquets et de filtrer ceux qui ne sont pas conformes à la politique en matière de sécurité de l'entreprise[4]. Le premier ne fait ainsi que surveiller, tandis que le second est à même d'exécuter des actions préventives visant à éviter l'incident.
- *DLP* : les outils de prévention de pertes de données (*data loss prevention*) visent comme le nom l'indique à éviter que des données ne soient perdues ou compromises par un accès indu de quelque manière que ce soit[5].
- *SIEM* : le système de gestion de l'information et des événements en matière de sécurité (*security information and event management*) analyse en temps réel le fichier des logs et des événements pour identifier tout comportement inhabituel[6].

Quels que soient les outils utilisés, il est important de documenter toutes les informations ayant trait à la découverte et à l'analyse de l'incident, parmi lesquels : (i) le statut de l'incident ; (ii) le résumé ; (iii) les indicateurs ; (iv) les incidents corollaires ; (v) les actions prises par les différents membres de l'équipe ; (vi) l'analyse de l'impact lié à l'incident ; (vii) les coordonnées des différentes parties impliquées ; (viii) la liste des preuves réunies durant l'analyse de l'incident et (ix) les prochaines étapes.

L'analyse de l'incident doit permettre de déterminer quel est l'impact fonctionnel sur la continuité des affaires et les efforts nécessaires pour rétablir la situation.

Si l'on suit la méthodologie retenue par le NIST[7], la classification en ce qui a trait à l'impact opérationnel est la suivante :

Catégorie	Définition
Aucun	Aucun impact quant à la capacité à conférer l'accès aux services aux utilisateurs
Faible	Tous les services sont encore disponibles, mais de manière moins efficiente
Moyen	Certains services critiques ne sont plus disponibles pour une partie des utilisateurs

Élevé	Certains services critiques ne sont plus disponibles pour aucun utilisateur

Quant aux efforts de remise en état, ce même NIST retient la classification suivante :

Catégorie	**Définition**
Normal	Temps de remise en état prévisible avec les ressources existantes
Supplémentaire	Temps de remise en état prévisible avec des ressources additionnelles
Important	Temps de remise en étant imprévisible ; des ressources additionnelles et une aide extérieure sont nécessaires
Irrécupérable	Remise en état impossible (données sensibles divulguées publiquement)

À l'issue de cette analyse, il conviendra d'apprécier quelles sont les personnes devant être informées de l'incident, parmi lesquelles : (i) le CIO ; (ii) le CISO (ces deux l'étant en principe d'ores et déjà) ; (iii) d'autres équipes de réponse en matière d'incident (approche décentralisée) ; (iv) le responsable du système ; (v) les ressources humaines ; (vi) les relations publiques et communication ; (viii) le service juridique.

d) Confinement, éradication et récupération

Une fois détecté et analysé, l'incident doit être traité.

Contenir l'incident est une phase essentielle pour minimiser son impact. Les stratégies en la matière varient. Ainsi sera-t-elle différente suivant que l'on a affaire à une attaque au travers d'un courriel vérolé ou d'une attaque par déni de service distribué (*DDoS*) qui touche au réseau. La décision à prendre dépend alors de la réponse apportée à plusieurs questions : (i) les systèmes touchés peuvent-ils être isolés des systèmes qui n'ont pas été affectés par l'incident (par exemple suppression du *malware*, déconnexion des comptes utilisateurs ayant fait l'objet d'un accès indu, etc.) ? ; (ii) une image du système touché a-t-elle pu être créée avant que quiconque n'y touche et sommes-nous assurés d'avoir un suivi documenté de toute personne susceptible d'intervenir et des démarches effectuées ?

Une fois l'incident maîtrisé, la question se pose de la restauration des systèmes affectés : (i) le système peut-il être restauré et nettoyé par diverses mesures pour éviter toute attaque

future (par exemple au travers du recours à des back-ups propres, remplacement de fichiers vérolés par des fichiers propres, installation de patches, changement de mots de passe, reconfiguration des firewalls et routeurs, etc.) ? ; (ii) la solution apportée est-elle durable ou faudra-t-il prendre de plus amples mesures à plus long terme ?

Les systèmes restaurés devront être régulièrement testés et surveillés pour s'assurer qu'ils ne risquent plus d'être affectés par un incident similaire à l'avenir. La question se pose alors de savoir quels outils la société a à sa disposition pour assurer un tel suivi.

e) Enseignements

Une fois l'incident clôturé, faire une séance de retour d'analyse fait partie des bonnes pratiques à mettre en place pour tirer les leçons du passé et éviter qu'il ne se reproduise, en répondant en particulier aux questions suivantes :

- que s'est-il passé exactement, et à combien de reprises ?
- la gestion de l'incident s'est-elle passée comme prévu ? Le plan a-t-il bien fonctionné et était-il adéquat ?
- quelle information aurait-il été utile d'avoir plus tôt ?
- les informations ont-elles bien circulé ?
- y a-t-il eu des démarches prises qui ont retardé le traitement de l'incident ?
- que ferait l'équipe différemment si un incident similaire devait se produire à l'avenir ?
- quelles mesures préventives sont susceptibles d'éviter qu'un incident comparable se produise à l'avenir ?
- à quels indicateurs faudrait-il en particulier prêter attention ?

III. Conclusion

La question de savoir quel doit être le degré de sophistication d'un plan de réponse et, corollairement, quelles ressources il convient de mettre en œuvre repose sur une analyse coûts-bénéfice.

En ce qui a trait aux entités soumises au RGPD, l'importance des sanctions administratives prononcées par les autorités en application de l'art. 83 RGPD plaident en faveur de l'octroi par les conseils d'administration d'un budget adéquat.

S'agissant des sociétés suisses qui ne sont soumises qu'à la Loi fédérale sur la protection des données, on peut se demander si cette analyse conduira au même résultat. Force est en effet

d'admettre que la révision n'a pas permis de conférer au Préposé fédéral des pouvoirs comparables à ceux accordés par le RGPD à ses pairs européens. Ainsi, seule une plainte pénale permettra à une autorité pénale de prononcer une amende pour le non-respect des mesures de sécurité préconisées par le Conseil fédéral dans une ordonnance à venir. Outre le fait que cette amende ne pourra pas dépasser le montant de CHF 250'000.–, elle sera de surcroît limitée aux seules infractions intentionnelles (art. 61 let. c nLPD). Difficile dès lors de faire moins dissuasif. Au final, l'incitation viendra donc certainement davantage de la prise de conscience du public et de la médiatisation de ces incidents par les médias, autant d'éléments susceptibles de créer un dommage réputationnel bien plus incitatif à prendre des mesures qu'une éventuelle amende bien théorique et éloignée. Sera-ce suffisant ? L'avenir le dira.

1. À ce sujet : Métille/Meyer, Annonce des violations de la sécurité des données, RSDA 2021, p. 23 ss.
2. Dans le modèle SANS, ces trois phases sont distinctes, de sorte que le modèle SANS est subdivisé en 6 phases, le modèle NIST – que je suis ici – n'en comportant que quatre. Pour une analyse de ces différences, voir : https://www.isacybersecurity.com/comparing-nist-sans-incident-frameworks/.
3. Pour des exemples de systèmes de détection d'intrusion (i) réseaux, par exemple : Snort, Bro, Suricata ou Enterasys ; (ii) hôtes, par exemple : AIDE, Chkrootkit, DarkSpy ou IceSword.
4. Pour des exemples de systèmes de prévention d'intrusion : CISCO IOS Intrusion Prevention System, Varonis.
5. Pour des exemples : Digital Guardian, Forcepoint, McAfee, Symantec, RSA, Endpoint Protector ou encore Protection des données CA (l'offre DLP de Broadcom).
6. Pour des exemples : LogRhythm, RSA, Splunk ou encore QRadar.
7. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800–61r2.pdf.

Proposition de citation : Philippe Gilliéron, L'établissement d'un plan de réponse en cas de faille de sécurité, 17 mai 2021 *in* www.swissprivacy.law/72

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.