WAVESTONE

RISKINSIGHT

LA LETTRE DES CONSULTANTS RISK MANAGEMENT ET CYBERSÉCURITÉ DE WAVESTONE

CYBER-RESILIENCE

UN NOUVEAU PILIER DE LA STRATÉGIE CYBERSÉCURITÉ

SOMMAIRE

DOSSIER

EDITO

Le début de l'été 2017 a montré très concrètement à quoi pouvait ressembler des cyberattaques mondiales, en particulier avec le cas de NotPetya. Les conséquences du *« ransomworm »* ne sont toujours pas terminées, le groupe Merck a annoncé fin novembre 2017 que cette cyberattaque lui coûtera plus de 600 millions de dollars en prévision sur l'exercice 2017 !

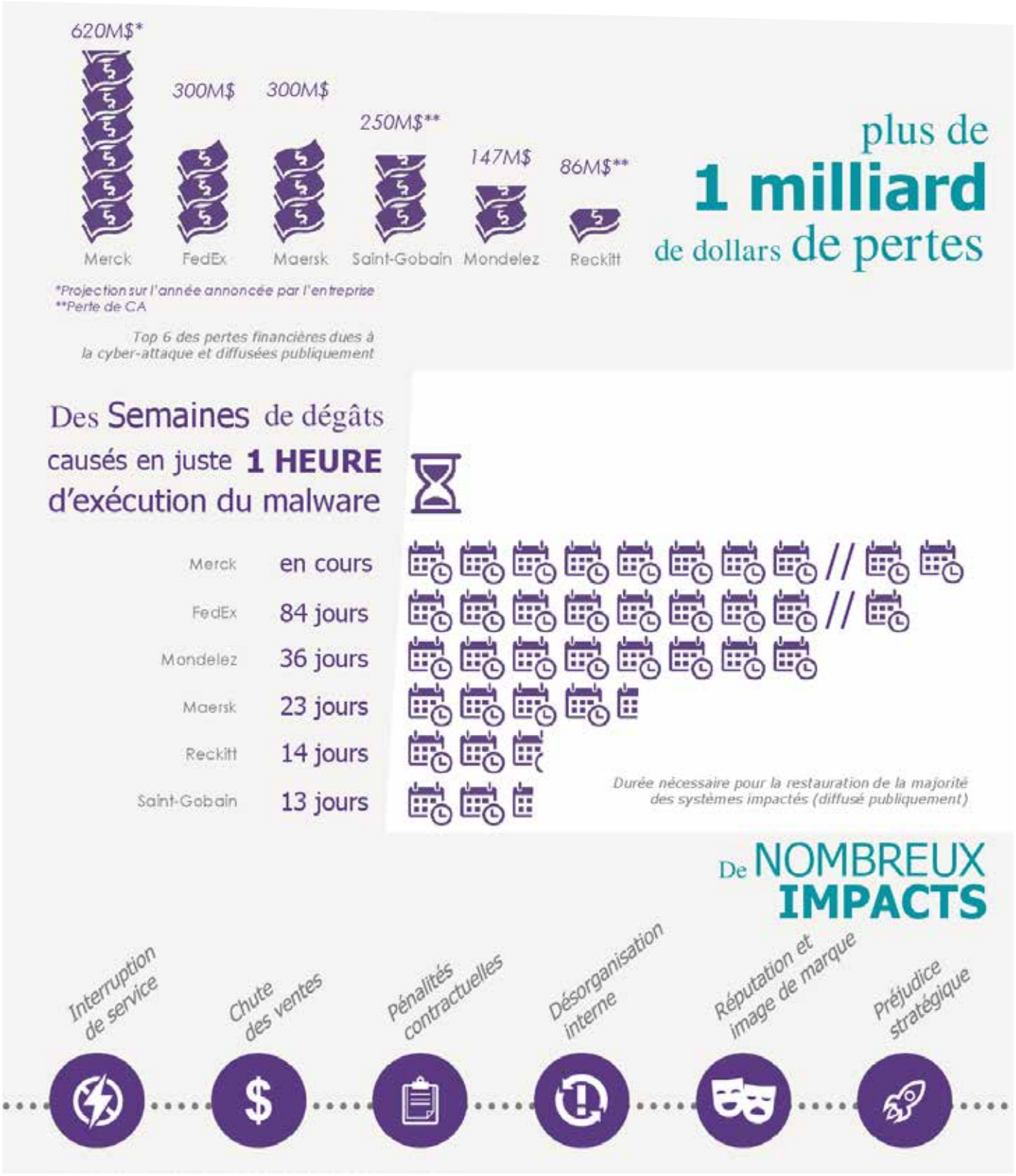
En additionnant les dernières annonces, le seuil des 2 milliards de perte est clairement en vue. C'est la première fois qu'un tel impact est recensé pour un incident cyber. Ce changement de dimension mobilise aujourd'hui les directions générales qui sont en attente sur les moyens de limiter les impacts de telles attaques mais aussi sur la posture à adopter lors d'un cas réel. Nous espérons que les articles ci-dessous vous aideront à y voir plus clair et à planifier les actions attendues.

Gérôme BILLOIS
Partner Cybersecurity & Digital Trust

NOTPETYA : 6 MOIS APRÈS, QUELS SONT LES IMPACTS ?

Gérôme BILLOIS, Partner
gerome.billois@wavestone.com

Denis BLANDIN, Consultant
denis.blandin@wavestone.com


620M$*
300M$
300M$
250M$**
147M$
86M$**
Merck
FedEx
Maersk
Saint-Gobain
Mondelez
Reckitt
plus de
1 milliard
de dollars de pertes
*Projection sur l'année annoncée par l'entreprise
**Perte de CA
Top 6 des pertes financières dues à la cyber-attaque et diffusées publiquement
Des Semaines de dégâts causés en juste 1 HEURE d'exécution du malware
Merck en cours
FedEx 84 jours
Mondelez 36 jours
Maersk 23 jours
Reckitt 14 jours
Saint-Gobain 13 jours
Durée nécessaire pour la restauration de la majorité des systèmes impactés (diffusé publiquement)
De NOMBREUX IMPACTS
Interruption de service
Chute des ventes
Pénalités contractuelles
Désorganisation interne
Réputation et image de marque
Préjudice stratégique

CYBER-RÉSILIENCE : LES ACTIONS CLES

Les attaques successives de Wannacry et NotPetya ont montré concrètement la fragilité des systèmes d'information et la capacité d'une menace cyber à rendre indisponibles pendant plusieurs semaines des parties importantes de systèmes assurant le bon fonctionnement d'une entreprise. Les sociétés touchées ont durement payé les conséquences de ces attaques. Qu'en retenir et comment mettre en place une stratégie de cyber-résilience efficace en cas de cyberattaques majeures ?

Face à une cyberattaque majeure, qu'elle soit destructive ou qu'elle entraîne une perte de confiance dans les systèmes clés, le premier réflexe pour une majorité d'entreprises est d'activer le plan de continuité d'activité (PCA). Celui-ci est un élément majeur de la stratégie de résilience des organisations ; afin d'en assurer la survie lorsque surviennent des sinistres d'ampleur entraînant l'indisponibilité de ressources informatiques, d'infrastructures de communication, d'immeubles voire de collaborateurs.

Or les cyberattaques majeures, destructives comme Wannacry ou NotPetya ou provoquant une perte de confiance dans les infrastructures (réseau, gestion des accès, gestion du parc…) comme les attaques ciblées en profondeur (APT), n'ont pas été prises en compte lors de l'élaboration de la majorité des PCA. Ces derniers, focalisés sur un enjeu de disponibilité, n'appréhendent pas les problématiques de la destruction simultanée et de la perte de confiance dans le SI induites par les cyberattaques.

En effet, les dispositifs de continuité du SI, le plus souvent liés aux ressources qu'ils protègent, sont également affectés par ces attaques. Depuis plus de dix ans, les dispositifs de continuité (utilisateurs ou informatiques) ont adopté les principes de mutualisation des infrastructures et de secours « à chaud » à la fois pour répondre aux exigences de reprise rapide et d'une meilleure exploitabilité. De fait, cette « proximité » entre le SI nominal et son secours rend vulnérables les dispositifs de continuité aux cyberattaques.

QUELLES VULNÉRABILITÉS POUR LES DISPOSITIFS DE CONTINUITÉ ?

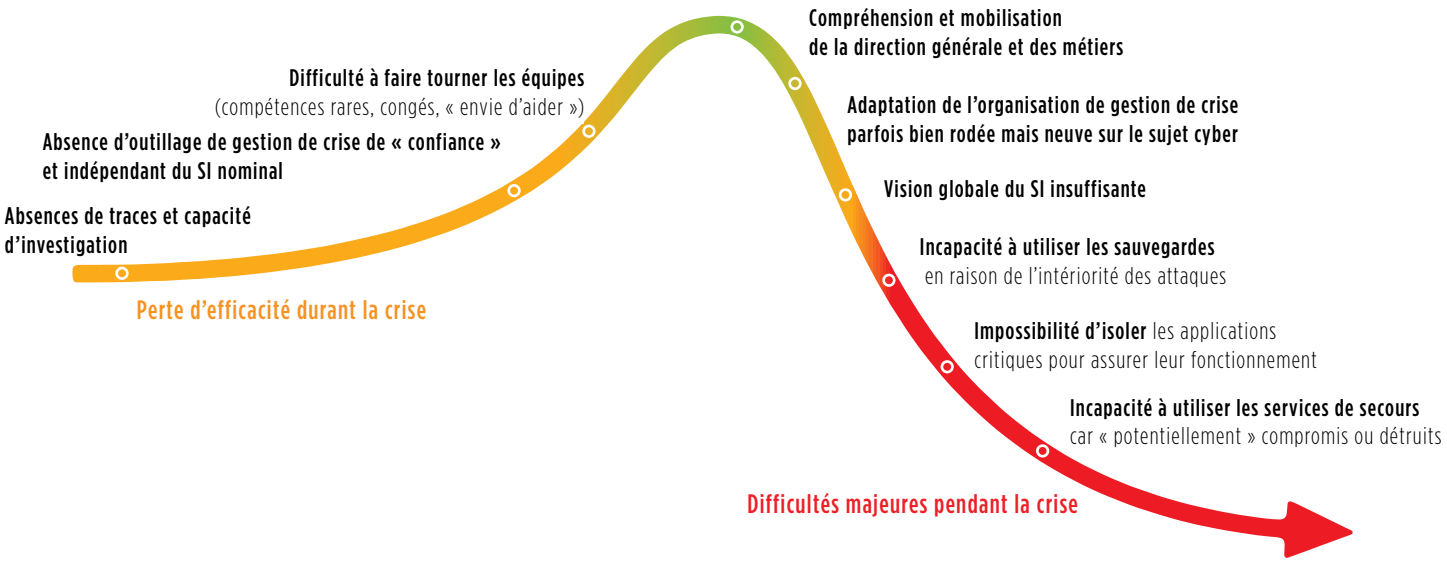
À titre d'exemple, lors d'une intervention de crise suite à l'attaque NotPetya, l'idée d'utiliser les postes de secours présents sur le site de repli a très rapidement été évoquée. Malheureusement ceux-ci avaient été détruits de la même manière que les sites nominaux car ils partageaient les mêmes systèmes de gestion de parcs et les mêmes vulnérabilités. Les investissements et les efforts investis dans les dispositifs de continuité ont semblé à ce moment très vains.

Enfin, les sauvegardes, établies sur une base souvent quotidienne, constituent pour la plupart des organisations le dispositif de dernier recours pour reconstruire le SI.

Malheureusement, en cas de compromission en profondeur, du fait de l'antériorité de l'intrusion (souvent plusieurs centaines de jours avant sa détection), ces sauvegardes embarquent de fait les éléments malveillants : malwares, camps de base, mais aussi les modifications déjà opérées par les attaquants. De plus, la continuité en tant que telle des systèmes de sauvegarde est souvent négligée. Lors de gestion de crise sur NotPetya, les serveurs gérant les sauvegardes ont eux-mêmes été détruits. Les restaurer a pris plusieurs jours vu leur complexité et leur imbrication dans le SI (nécessité de disposer d'un ActiveDirectory pour lancer des restaurations alors que la sauvegarde de l'AD était nécessaire pour le reconstruire, reconstruction de l'index des bandes de sauvegardes détruit avec le reste…).

S'agissant des SI industriels, les constats sont tout aussi manifestes. Les systèmes numériques industriels sont résilients à des pannes techniques ou des incidents mécaniques anticipés. En revanche, ils n'ont que rarement intégré, dès leur conception, les potentialités d'une malveillance humaine et ne disposent souvent pas de mécanismes de sécurité avancés. Du reste, leur cycle de vie long (plusieurs dizaines d'années) les expose à l'exploitation de vulnérabilités parfois anciennes. Enfin l'indépendance des chaînes de contrôle (Systèmes Instrumentés de Sécurité, cf. encadré ci-après) vis-à- vis des systèmes numériques qu'elles supervisent n'est pas toujours appliquée.

Principaux écueils rencontrés lors de la gestion de crise cyber



DES SCÉNARIOS D'ATTAQUES MAJEURES ILLUSTRÉS PAR DES ATTAQUES RÉCENTES

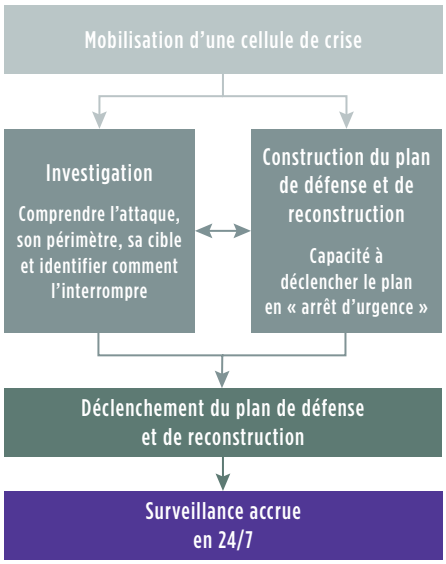
La destruction logique ou l'indisponibilité d'une grande partie du système d'information

Concrétisé par les attaques de vrai-faux rançongiciels Wannacry et NotPetya, ce type d'attaque entraîne une indisponibilité massive du fait du chiffrement des fichiers de données et/ou du système d'exploitation. Les sociétés touchées par ce type d'attaque (Merck, Maersk, Saint Gobain, Fedex… mais aussi Sony Pictures ou Saudi Aramco) ont perdu jusqu'à plus de 95% de leurs systèmes d'information (des dizaines de milliers d'ordinateurs et de serveurs) en un délai souvent inférieur à 1h. La situation au démarrage de la crise est très difficile car il n'y a plus aucun moyen de communication et d'échange au sein de l'entreprise, y compris au sein de la DSI. Les victimes ont communiqué sur des pertes de plusieurs centaines de millions d'euros suite à ces attaques.

La compromission et la perte de confiance dans le système d'information

Il s'agit d'attaques ciblées qui ne remettent en pas en cause le bon fonctionnement du système mais qui visent à donner aux attaquants l'accès à l'ensemble des systèmes de l'entreprise (messagerie, fichiers, applications métiers…), leur permettent d'usurper l'identité de n'importe quel employé et de réaliser des actions en leur nom. Les attaquants peuvent ainsi exfiltrer tout type de données ou réaliser des actions métiers demandant plusieurs validations successives. Ces attaques ont touché de très nombreuses entreprises dans tous les secteurs avec comme conséquences des fraudes massives, comme celles ayant touché la banque du Bangladesh, ou des vols de données financières et de paiements comme celles ayant touchés plusieurs groupes de distribution aux Etats-Unis dont Target ou encore Home Depot. La situation au démarrage de la crise est complexe en raison d'une conjugaison de plusieurs éléments aggravants : perte de confiance dans le système d'information et flou grandissant sur les actions et objectifs. Il s'agit alors d'investiguer discrètement jusqu'à pouvoir déloger l'attaquant et reconstruire un système sain. Les victimes touchées par ces attaques ont fait état d'impacts financiers de plusieurs centaines de millions d'euros.

Méthodologie de gestion d'une crise cyber



MUSCLER LA GESTION DE CRISE

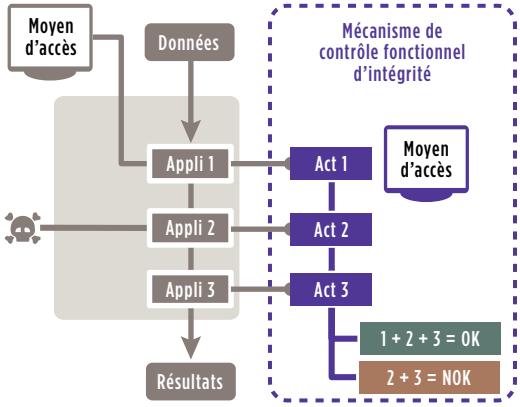
Les crises cyber sont des crises particulières : souvent longues (plusieurs semaines), parfois difficiles à cerner (qu'a pu faire l'attaquant ? depuis combien de temps ? quels sont les impacts ?) et impliquant des parties externes elles-mêmes souvent peu préparées sur ce sujet (avocats, huissiers, autorités, fournisseurs, voire les clients…). Il est donc nécessaire d'ajuster les dispositifs existants qui n'ont pas été conçus pour intégrer la dimension cyber.

Acteur opérationnel de la gestion de la crise cyber, la DSI ne doit pas être sur-mobilisée sur l'investigation et la défense au détriment de la production et du secours. Cet aspect constitue un point d'anticipation important à ne pas négliger. Il s'agira donc d'identifier clairement les équipes à mobiliser sur la crise et d'organiser les interventions parallèles d'investigation et de construction de plan de défense.

Au-delà de l'aspect organisationnel, il faudra s'assurer de disposer également de l'outillage d'investigation (cartographie, recherche de signature de l'attaque, SI de gestion de crise indépendant, capacité d'analyse de malware inconnu…), d'assainissement (capacité de déploiement rapide de correctifs ou de « vaccin », isolation en urgence de portions non touchées du SI, isolation réseau…) et de reconstruction (accès rapide aux sauvegardes, accès aux documentations minimum de reconstruction, support des fournisseurs clés sur le SI, capacité à réinstaller massivement des postes de travail…) requis pour comprendre la position de l'attaquant, stopper sa propagation et faire repartir au plus vite l'activité.

La définition d'un guide de gestion de crise, définissant les étapes structurantes, les responsabilités macroscopiques et les points de clés de décision sera un plus. Et parce qu'il est primordial de s'exercer en amont afin d'être prêt le jour où il faut faire face à la crise, la réalisation d'exercice de crise sera un bon révélateur de la situation réelle.

Mécanisme de contrôle fonctionnel d'intégrité



Mécanisme de réconciliation indépendant du processus applicatif pour détecter une possible compromission dans la chaîne des actes fonctionnels métiers ou techniques

Exemples

- Élévation du plafond de découvert autorisé sur un compte sans passer par le back office bancaire
- Création d'un compte administrateur AD sans création d'un ticket dans les outils de ticketing support

REPENSER LES DISPOSITIFS DE CONTINUITÉ

Les dispositifs de continuité doivent également évoluer pour s'adapter aux menaces cyber. Les solutions possibles sont nombreuses et peuvent toucher tous les types de dispositifs de continuité. Le plan de reprise utilisateur peut intégrer par exemple la mise à disposition de clés USB avec un système alternatif. Les collaborateurs pourraient l'utiliser en cas de destruction logique de leur poste de travail.

Certains établissements ont fait le choix de provisionner des volumes de postes de travail de remplacement directement avec leurs fournisseurs de matériel afin de les délivrer rapidement en cas de destruction physique.

Le plan de continuité informatique peut inclure de nouvelles solutions pour être efficace en cas de cyberattaque. La plus emblématique vise à construire des chaînes applicatives alternatives. Il s'agit de « dupliquer » une application sans utiliser les mêmes logiciels, systèmes d'exploitation et équipes de production. C'est une solution extrême, très coûteuse et difficile à maintenir, mais qui est envisagée pour certaines applications critiques dans le monde de la finance (notamment les infrastructures de paiement à caractère systémique).

D'autres solutions moins complexes sont envisagées. Il s'agit par exemple de l'ajout de contrôle fonctionnel d'intégrité dans le processus métier. Son concept repose sur la réalisation de contrôles réguliers, à différents niveaux et à différents endroits dans la chaîne applicative (*« multi-level controls »*). Ceci permet de détecter rapidement des attaques qui toucheraient par exemple les couches techniques (modification d'une valeur directement dans une base de données) sans avoir été réalisées par les actions métier classiques (via les interfaces graphiques). Ces mécanismes peuvent aussi s'appliquer aux systèmes d'infrastructures, par exemple en réconciliant les tickets de demande de création de compte d'administration avec le nombre de comptes réellement dans le système.

D'un niveau de complexité intermédiaire, il est possible d'envisager la définition de zone d'isolation système et réseau (*« floodgate »*) que l'on peut activer en cas d'attaques et qui vont isoler les systèmes les plus sensibles du reste du SI. Le SI industriel pourra, à ce titre, constituer à lui seul, une de ces zones d'isolation vis-à-vis du reste du SI.

Ces évolutions, souvent majeures, doivent s'inscrire dans une revue des stratégies de secours existantes afin d'évaluer leur vulnérabilité et l'intérêt de déployer des nouvelles solutions de cyber-résilience, en particulier sur les systèmes les plus critiques. L'évolution des Business Impact Analysis (BIA) pour inclure cette dimension est certainement une première étape clé.

Exemples d'actions dans une stratégie de cyber-résilience

ANTICIPER POUR NE PAS ROMPRE

Introduire de la diversité et de la souplesse
(postes utilisateurs, infrastructures, applicatifs, fournisseurs tiers…)

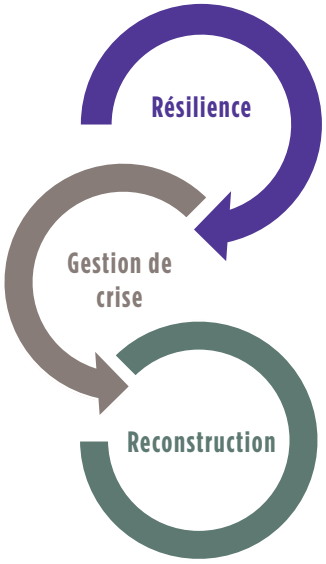
Limiter les effets d'amplification d'une attaque (durcir, cloisonner…)

Refondre son plan d'alerte et de continuité
(prioriser, s'entraîner…)

RECONSTRUIRE VITE ET SAIN

Valider l'innocuité / la solidité
(Réaliser des investigations numériques …)

Massifier la reconstrution
(Relancer rapidement les services non-touchés, paralléliser, s'appuyer sur les collaborateurs…)



AGIR RAPIDEMENT ET EFFICACEMENT

S'organiser et pouvoir travailler
(Structurer les cellules de crise, gérer les relations avec les autorités, mobiliser l'expertise, disposer de moyen télécoms de secours…)

Comprendre et sauver ce qui peut l'être
(Disposer de traces, investiguer, identifier et immuniser…)

SANS CYBERSÉCURITÉ, LA CYBER-RÉSILIENCE N'EST RIEN

Implémenter ces nouvelles mesures de cyber-résilience nécessite des efforts importants. Des efforts qui seront vains si ces solutions de secours et les systèmes nominaux ne sont pas eux-mêmes déjà sécurisés correctement et surveillés avec attention. Le RSSI est l'acteur clé pour faire aboutir ces démarches souvent entamées mais rarement finalisées. L'aide du *Risk Manager* (RM) — ou, s'il est désigné, son Responsable du Plan de Continuité d'Activité (RPCA) — sera alors un plus. Il est aujourd'hui communément acquis qu'il est impossible de sécuriser des systèmes à 100%, il faut donc accepter la probabilité d'occurrence d'une attaque et c'est à ce moment-là que le RM ou son RPCA prendra tout son rôle.

Gérôme BILLOIS, Partner
gerome.billois@wavestone.com

Frédéric CHOLLET, Senior Manager
frederic.chollet@wavestone.com

LA CRISE CYBER, UN SUJET MÉDIATIQUE À PART ENTIÈRE

Bien qu'elles s'appuient sur des objectifs, des méthodes et des outils similaires, gestion et communication de crise cyber s'approprient nécessairement les spécificités des problématiques qu'elles traitent pour être pertinentes et donc efficaces. Dans le cas d'une crise d'origine cyber, la prise en compte de ses particularités et de son exposition à des publics parfois nombreux, exige une anticipation et une préparation spécifiques dont la première étape est la compréhension de l'exposition médiatique qu'elle aura.

ADRESSER LE BESOIN DE SAVOIR ET LE BESOIN DE RASSURANCE

Soutenue par l'augmentation du nombre d'incidents et d'attaques sur les systèmes d'information, la crise cyber s'est installée dans l'espace public. La démocratisation de son champ lexical est ainsi un indicateur marquant de la place médiatique qu'a pris ce sujet. Fuite de données, ransomware, hacktiviste, DDoS, phishing, lanceur d'alerte, ces mots ont quitté les salles serveurs et les blogs spécialisés pour se faire une place dans les colonnes des journaux nationaux et dans le vocabulaire de la plupart des français. La crise cyber n'est plus un simple incident qualité silencieusement traité en interne et est devenue un événement qui suscite l'intérêt de tous les publics entraînant mécaniquement dans son sillage une crise de nature communicationnelle. Cependant, si la popularité nouvelle de cette thématique se décline logiquement dans l'accroissement de la couverture de ces crises, d'autres éléments justifient l'augmentation significative des sollicitations, qu'elles soient internes ou externes à l'organisation en crise.

Lorsque la crise cyber a pour conséquence la fuite d'une donnée par exemple, ce n'est plus seulement le sujet de la crise qui est médiatique, mais son objet même. De fait, lorsque la donnée fuite ou est volée, sa nature intrigue et suscite la curiosité, qu'il s'agisse d'une donnée personnelle, d'un secret d'état ou simplement d'une conversation privée. Cette mécanique engendre logiquement pour de nombreux publics tant le besoin de connaître l'inconnu, que de s'assurer de ne pas en être la victime. Ces deux besoins primaires de curiosité et de réassurance constituent les moteurs essentiels de la couverture médiatique et plus généralement incite le consommateur d'information, le partenaire, le client à combler ce besoin et à chercher à obtenir cette information. La même logique suppose que la source de cette information, en l'occurrence, le détenteur légitime de cette donnée adresse ces requêtes et communique sur l'incident.

Que ce soient des évènements stratégiques tels que des élections présidentielles ou des conversations privées du quotidiens via des médias digitaux qui sont compromis, l'effet médiatique de la crise se voit amplifié par le caractère extraordinaire de l'événement. Cela résulte tant de sa supposée impossibilité que de la confiance que le public lui confère. La rupture soudaine de la confiance placée en ces « institutions » d'importances majeures, érigées en bonne place dans une version 2.0 de la pyramide de Maslow, génère alors elle aussi l'intérêt et le besoin de savoir, traduits dans une explosion du nombre des requêtes et des demandes d'information à l'organisation en crise.

Figure 1 : Exemple de pyramide de Maslow

GUERRE DE COMMUNICATION ENTRE L'ATTAQUANT ET LE COMMUNICANT

La communication de crise cyber est ainsi un exercice particulier de par le sujet qu'elle traite, mais aussi de par la nature des acteurs en présence. De fait, quand des sommes incommensurables d'argent sont dérobées sans coup férir ou que des institutions tombent sous les attaques d'hacktivistes « citoyens », l'opinion voue une sympathie relative à l'encontre du héros moderne qu'est le pirate romanesque, le *hacker* hors la loi, le justicier anonyme.

Ce personnage public, conscient de son image et des codes du monde communicationnel, saura bien entendu se jouer de cet environnement. Ainsi, les méthodes mêmes des attaquants renforcent la place centrale de la communication dans la gestion des crises cyber. Les attaques aux motifs politiques, idéologiques et militants ne se limitent plus à la compromission d'un système mais envoient un message dont la publicité doit être maximale.

Cette appropriation manifeste des méthodes propres aux activistes s'illustre de plusieurs manières : Annonce d'un DDoS en amont, défacement d'un site internet, publication au fur et à mesure de preuves d'un vol sur les réseaux sociaux, diffusion d'informations telles que des échanges de conversations mails privés compromettants… Si les attaquants ont appris à maximiser l'impact réputationnel des attaques, ils utilisent aussi ce levier afin de perturber la gestion de crise de leur cible et générer un bruit qui leur fera gagner du temps une fois leur attaque découverte. Alors qu'un des facteurs clefs du succès d'une gestion de crise est la reprise en main du rythme de celle-ci et de la publication de nouveaux éléments, la crise cyber laisse inéluctablement ce pouvoir à un tiers malveillant.

Ce tiers peut aussi, si la compromission est profonde, altérer les moyens de communication de l'entreprise. Alors qu'elle tente de répondre à la nécessité de s'exprimer urgemment et largement, cette entrave peut lourdement affecter la fluidité de sa communication. Sans messagerie mail, comment diffuser un message à ses employés ? Sans réseaux sociaux, comment être au plus proche de sa communauté et répondre à ses questions ?

RESTAURER LE RAPPORT DE CONFIANCE PAR LA COMMUNICATION

Fasciné par les attaquants et l'ampleur des attaques, le grand public n'en demeure pas moins intransigeant à une heure où la confiance et la donnée constituent la valeur même d'une entreprise. Intrinsèquement, la préservation de la première suppose la protection de la seconde. Lorsque l'organisation faillit à cet objectif, la communication de crise est seule en mesure de restaurer ce rapport de confiance duquel dépend l'avenir de la relation avec clients et partenaires qui continueront ou non à confier la garde de leurs données ou la gestion de leurs outils, ainsi que leurs services à une organisation.

Cette exigence de confiance entraine par ailleurs, lorsqu'elle est brisée, la recherche et la désignation rapide d'un responsable. Bien que la réalité des faits soit bien plus complexe, le grand public aura aisément tendance à supposer que les attaques informatiques sont rendues possibles par l'exploitation d'une vulnérabilité et donc d'une faute.

Une fuite de données, n'est ainsi pas uniquement perçue comme une attaque perpétuée par un tiers malintentionné, mais aussi comme une négligence dans la défense de l'entreprise victime du vol. Cette dernière se voit automatiquement désignée comme responsable et sa réputation en est logiquement impactée. Alors même que les attaquants se professionnalisent, que les attaques se complexifient et que l'absence de vulnérabilité est un mythe, la cyberattaque est aujourd'hui un sujet de gestion et de communication de crise à part entière. Du fait de son impact potentiel sur le quotidien du grand public et donc sa nature médiatique, elle force la victime, considérée comme co-responsable de sa perte, à s'exprimer.

RÉALISER L'EFFORT DE SIMPLICITÉ POUR MIEUX COMMUNIQUER FACE À LA CRISE

Au-delà de la définition d'une stratégie claire, partagée et opportune, la gestion de crise cyber avec son rythme particulier et les entraves causées par les attaquants doit être accompagnée d'une communication particulière qui suppose enfin un dernier travail : l'effort de simplicité.

Face à la crise cyber et comme pour tout type de crise, communiquer suppose d'être en mesure de traduire les évènements subis et les actions correctives menées en impacts clairs et de porter ce discours de façon cohérente. Bien entendu, la complexité des termes et des rouages d'une crise cyber rend cet exercice délicat et constitue une autre spécificité à prendre en considération.

Dans ce cadre, par sa capacité à traduire la cause technique en conséquence métier et plus généralement par son pouvoir vulgarisateur, le rôle du RSSI et de ses équipes est central. En situation nominale comme en temps de crise, la mission du RSSI est de porter cet effort de traduction des faits et des composantes techniques non seulement en impacts métiers mais en impacts compréhensibles et convaincants pour des publics diversifiés et non experts. Il ou elle peut ainsi être amené à concevoir, voire à porter les éléments de langage de communication de crise de la même manière qu'un représentant des ressources humaines sera exposé lors d'une crise sociale.

Sans présupposer de son exposition au journal télévisé d'une grande chaine de télévision, la parole des experts SI sera attendue sur les réseaux sociaux, sur les réseaux professionnels, dans la presse spécialisée ou en interne. En communication de crise, chacun est responsable de tous et tout un chacun doit s'y préparer.

Ainsi, le sujet cyber porte une puissance médiatique qui lui est propre ; dont la conséquence immédiate est l'augmentation considérable des attentes et des demandes d'informer émanant des différentes directions d'une organisation ainsi que du public externe. Si l'imminence de l'occurrence d'un incident SI implique une défense spécifique et une planification de la continuité des opérations, elle exige aussi l'anticipation de ces requêtes et une préparation active à cet effort global de communication.

Swann LASSIVA, Consultant
swann.lassiva@wavestone.com

LE CLOUD, LA FIN OU RENOUVEAU DU SECOURS INFORMATIQUE ?

Les entreprises ont de plus en plus recours aux services cloud (SaaS, PaaS, IaaS) pour leur environnement informatique. Ils apportent plus de flexibilité avec des coûts pouvant être plus avantageux qu'une infrastructure classique. En 2016, en France, 48% des entreprises de plus 250 personnes y avaient recours soit une augmentation de 12 points par rapport à 2014. La plus grande disponibilité des infrastructures Cloud est souvent identifiée comme une opportunité. Néanmoins, le risque de défaillance d'un datacenter du fournisseur n'est que rarement traité, alors que ses services reposent sur des datacenters bien physiques et non pas sur des nuages. Ces datacenters font face aux mêmes menaces que les « datacenters traditionnels » : catastrophes naturelles, erreurs humaines…

Il est donc nécessaire de se demander comment assurer le secours informatique de ces infrastructures Cloud.

LE SECOURS INFORMATIQUE SAAS, UNE RESPONSABILITÉ DU FOURNISSEUR À FORMALISER

Un service SaaS (*Software as a Service*) est un logiciel mis à disposition et directement consommable depuis Internet. Il est géré et administré par un ou plusieurs fournisseurs. Le client n'a donc pas la latitude nécessaire pour opérer le secours (pas d'accès aux données brutes, pas d'accès aux codes sources, ni aux applicatifs pour dupliquer l'infrastructure…), il doit donc s'en remettre au bon vouloir de son fournisseur.

Un niveau de couverture du secours informatique pour SaaS variable suivant la maturité du fournisseur

Trois grandes tendances se dessinent :

- **Les fournisseurs qui disposent d'un plan de secours informatique inclus**
  Dans le cadre de l'offre standard, le fournisseur assure un secours sur un datacenter distant, complété généralement par des sauvegardes externalisées. Il ne s'engage néanmoins que rarement sur les délais de reprise. Ex : les grands acteurs du SaaS (ex : Office 365, SalesForce, SAP…) , ainsi que certains acteurs de taille intermédiaire (ex : Evernote, Xero…) ;
- **Les fournisseurs qui disposent simplement d'une sauvegarde externalisée**
  En tant que tel, aucun plan de secours informatique n'est clairement établi. Le client doit alors s'interroger sur la capacité du fournisseur à restaurer les sauvegardes en cas de sinistre global sur le site principal. Ex : Des fournisseurs de taille intermédiaire (ex : Zervant, Sellsy…) ;
- **Les fournisseurs qui ne communiquent pas ou n'en disposent pas**
  Le sujet du secours informatique n'est pas abordé, il est donc préférable de considérer que rien n'est fait. Ex : Les acteurs de petite taille sont généralement dans ce cas.

L'importance de l'aspect contractuel

Dans la très grande majorité des cas, les fournisseurs SaaS ne s'engagent pas dans leur contrat sur leur façon de gérer le secours ; même lorsque ceux-ci mettent en avant leur capacité à traiter cette problématique. En effet, les contrats comportent généralement par défaut des clauses de Force Majeure stipulant que le fournisseur n'est pas responsable de manquement aux obligations du contrat dans la mesure où ce manquement est causé par un évènement en dehors de leur contrôle raisonnable. Le risque juridique doit donc être traité lors de la souscription et ces clauses supprimées pour s'assurer un bon niveau de couverture.

Lors de la souscription, comme pour des contrats classiques, les clients doivent s'assurer que figure bien des engagements de service, en particulier pour les secours informatiques :

- Le **délai de reprise** (Durée Maximale d'Interruption Acceptable ou DMIA) et les pertes de données(Perte de Données Maximale Acceptable ou PDMA) en cas de sinistre;
- Le **plan de secours informatique du fournisseur** incluant les modalités de gestion de crise ainsi que l'obligation de conduire plusieurs **tests probants** par an de ce plan avec la possibilité pour le client d'accès au rapport des tests ;
- Les **pénalités financières** et le droit de résilier le contrat (avec en particulier la récupération des données exploitables) en cas de manquement aux engagements.

LE SECOURS INFORMATIQUE DU IAAS/ PAAS, UNE MISE EN OEUVRE ET UNE RESPONSABILITÉ DU CLIENT

Le IaaS (*Infrastructure as a Service*) est une offre standardisée et automatisée de ressources de calcul, de moyens de stockage et de ressources réseau détenus et hébergés par un fournisseur et mis à disposition au client à la demande. L'offre PaaS (*Platform as a Service*) est similaire à celle du IaaS, à la différence près qu'elle ne concerne que les infrastructures applicative (définitions Gartner) Contrairement au cas du SaaS, le secours reste sous la responsabilité du client dans les deux cas : les fournisseurs IaaS/ PaaS mettent à disposition des ressources dans différents datacenters et le client est responsable de l'usage et de la configuration qu'il en fait. Deux solutions s'offrent aux clients utilisant ces services : confier à un prestataire son secours ou bien le gérer lui-même.

Avoir recours à un prestataire de secours, un marché peu mature

Les prestataires de secours dans le Cloud sont désignés par l'acronyme *« DRaaS »* pour *Disaster Recovery as a Service*. Initialement, les fournisseurs DRaaS proposaient d'assurer dans le Cloud le secours de votre SI « on-premise ». Mais ils proposent également aujourd'hui d'assurer le secours de vos infrastructures déjà dans le Cloud, AWS ou Azure par exemple. La maturité reste très variable selon les fournisseurs et le cloud utilisé. Certains fournisseurs DRaaS imposent que le Cloud de destination du secours soit le leur, ne permettant pas ainsi de couvrir le secours de service PaaS.

Comme avec le SaaS, **pas de garanties incluses par défaut** quant aux pertes de données ou au délai de reprise, il faut les négocier. Les fournisseurs promettent de pouvoir s'adapter aux exigences du client ! Pour s'assurer que le secours fonctionne, le client doit prévoir la réalisation régulière **de tests probants du secours** (recommandation d'une fois par an).

Réaliser soi-même son secours en utilisant les outils proposés par le fournisseur

Comme sur une infrastructure *« on-premise »*, il est nécessaire de réfléchir et définir sa stratégie de secours dès la conception. Cette stratégie doit intégrer la capacité de réaliser des tests probants permettant d'assurer un niveau de confiance suffisant dans son plan.

La mise en place est simplifiée par les outils mis à disposition par les fournisseurs Cloud et la forte standardisation des environnements Cloud. Les grands acteurs publient dans des livres blancs les grandes lignes directrices pour mettre en place un tel projet (par exemple AWS ou Azure).

Les concepts des stratégies du secours informatique restent proches de celles pour les datacenters on-premise.

On peut en dénombrer quatre principales :

- **la sauvegarde et restauration** : simple sauvegarde des données et images des machines sur un site distant, restaurées en cas de sinistre ;
- **la veilleuse** : réplication des bases de données et mise à disposition des machines sous forme d'images prêtes à être démarrées en cas de sinistre ;
- **le secours à chaud :** réplication complète du site primaire (données et machines), le site de secours est sous-dimensionné en termes de performances et est prêt à monter en charge en cas sinistre ;
- **le multi site (ou actif-actif)** : les deux sites sont identiques et se partagent la charge des utilisateurs. En cas de sinistre, le site restant peut monter en charge pour accueillir la totalité des utilisateurs.

Des solutions hybrides pouvant mieux s'adapter aux exigences de délai de reprise, coût et complexité de la solution peuvent être envisagées.

Le véritable apport du Cloud pour le secours concerne les nombreux outils mis à disposition simplifiant la mise en œuvre et le déclenchement.

La réplication des données est ainsi simplifiée pour les options de géo-réplication asynchrones (plusieurs copies répliquées dans d'autres régions). La PDMA est variable en fonction des types de données et des outils proposés. Au-delà de cette option, une redondance locale des données est presque systématiquement incluse.

La forte standardisation permet également d'automatiser la reprise : les scripts ou API mis à disposition par les fournisseurs permettent d'automatiser le déploiement des infrastructures, le redimensionnement des instances en fonction de métriques précédemment définies, la répartition des charges et du trafic ou, l'adressage IP etc... afin d'accélérer de façon significative l'activation d'un site de secours.

Les outils de surveillance et alerte qui sont également proposés visent à faciliter le Maintien en Conditions Opérationnelles (MCO) du secours et peuvent être utilisés pour détecter au plus tôt un incident voire, dans certains cas, automatiser partiellement le déclenchement du secours.

Enfin la capacité à provisionner des nouvelles ressources en quelques minutes permet de limiter l'OPEX. **A stratégie équivalente, il est ainsi possible d'avoir des gains de 40 à 70% sur le coût du secours !**

Vers une plus grande prise en charge par le fournisseur ?

Azure prévoit une option, courant 2017, pour assurer le secours des machines virtuelles hébergées au sein de leur plateforme via la complétion de leur service *« Site Recovery »*. En effet, *« Site Recovery »* propose à l'heure actuelle de prendre en charge le secours de site traditionnel en utilisant le cloud Azure pour accueillir le site secondaire, mais Microsoft souhaite étendre ce service au secours de leurs propres infrastructures. Cet outil permettrait un déploiement automatique du site secondaire (de type actif-passif), une réplication automatique des données et une mise en place de tests facilitée.

Cette option est passée en *« public preview »* fin mai 2017. Un projet équivalent n'est pas d'actualité chez les autres principaux fournisseurs IaaS/PaaS.

LE CLOUD FACE AU RISQUE SYSTÉMIQUE DES FOURNISSEURS

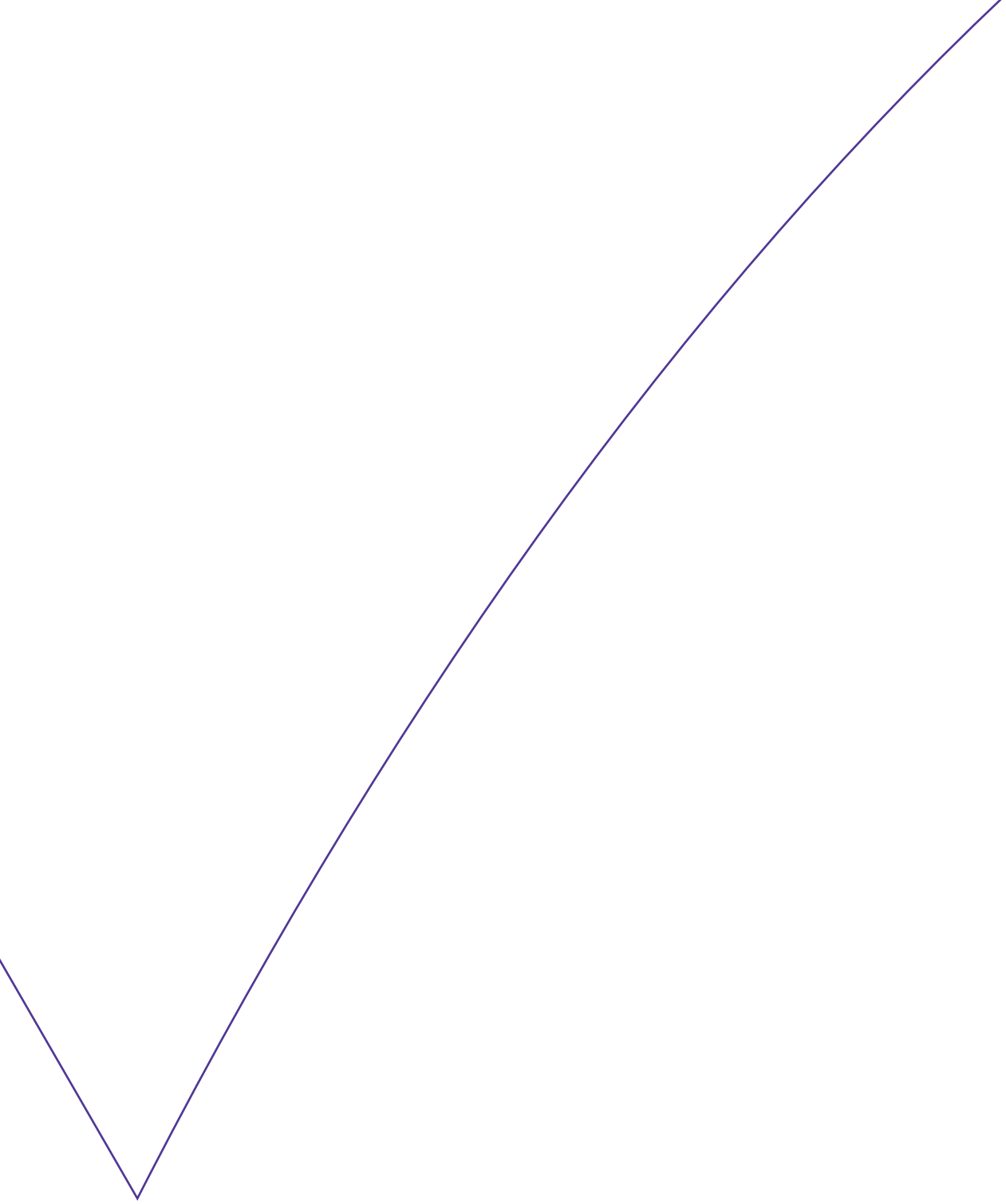
Le secours informatique des services hébergés dans le cloud s'aborde différemment selon le type de service utilisé. Le secours du SaaS doit être géré contractuellement et est sous la responsabilité du fournisseur tandis que le secours du IaaS/PaaS, simplifié par les outils, reste sous la responsabilité du client.

Le risque de défaillance généralisé d'une région d'hébergement d'un fournisseur existe comme le montre les derniers incidents. Même si aujourd'hui, les incidents ont été de courte durée ou avec des impacts fiables, une défaillance généralisée ne peut pas être ignorée. Reste donc à traiter la problématique de cyber-résilience. L'utilisation d'un 2ème fournisseur cloud permet de couvrir le risque de destruction ou d'indisponibilité majeure des infrastructures du premier. Cette solution reste très complexe car la portabilité d'un fournisseur à un autre est délicate. Pour l'instant, peu d'entreprises s'y sont risquées, même si l'on peut citer l'exemple de Snapchat qui utilise le cloud Google pour sa production et prévoit d'utiliser celui d'Amazon pour son secours d'ici à 5 ans.

Etienne LAFORE, Manager
etienne.lafore@wavestone.com

Lesly MERINE, Senior Consultant
lesly.merine@wavestone.com

Valentin LEMENUT, Consultant
valentin.lemenut@wavestone.com



Responsable de la publication : Frédéric GOUX
Rédacteur en chef : Gérôme BILLOIS
Contributeurs : Denis BLANDIN, Frédéric CHOLLET,
Swann LASSIVA, Etienne LAFORE, Lesly MERINE, Valentin LEMENUT
ISSN 1995-1975

WAVESTONE

www.wavestone.com

Wavestone est un cabinet de conseil, issu du rapprochement de Solucom et des activités européennes de Kurt Salmon (hors consulting dans les secteurs retail & consumer goods en dehors de France).

La mission de Wavestone est d'éclairer et guider ses clients dans leurs décisions les plus stratégiques en s'appuyant sur une triple expertise fonctionnelle, sectorielle et technologique.

Fort de 2 500 collaborateurs présents sur 4 continents, le cabinet figure parmi les leaders indépendants du conseil en Europe et constitue le 1er cabinet de conseil indépendant en France.