WAVESTONE

CYBER-RÉSILIENCE

PLIER POUR NE PAS ROMPRE

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 indisponible pendant plusieurs semaines des parties importantes des systèmes assurant le bon fonctionnement des entreprises. Les sociétés touchées ont durement payé les conséquences de ces attaques. Qu'en retenir et comment se préparer pour résister et réagir efficacement 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.

AUTEURS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

FRÉDÉRIC CHOLLET
frederic.chollet@wavestone.com

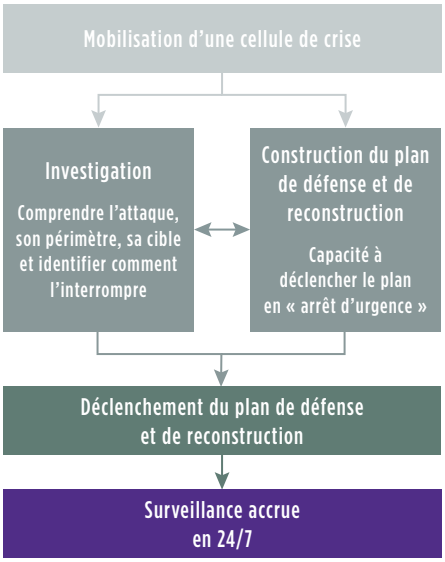
A titre d'exemple, lors d'une intervention de crise suite à l'attaque NotPetya, l'idée d'utiliser les postes de secours présents sur le site de repli a très rapidement été évoquée. Malheureusement ceux-ci avaient été détruits de la même manière que les sites nominaux car ils partageaient les mêmes systèmes 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 inutiles.

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.

Méthodologie de gestion d'une 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 communications et d'échanges an 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.

MUSCLER LA GESTION DE CRISE

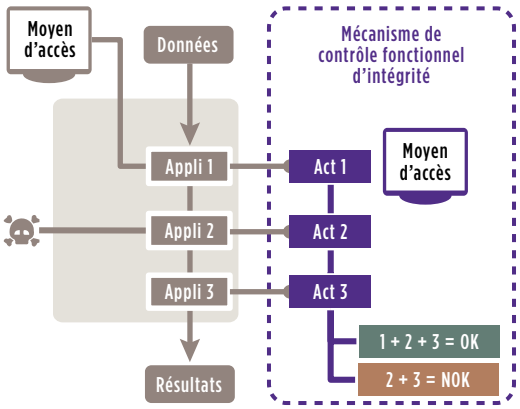
Les crises cyber sont des crises particulières : souvent longues (plusieurs semaines), parfois difficiles à cerner (qu'a pu faire l'attaquant ? depuis combien de temps ? quels sont les impacts ?) et impliquant des parties externes elles-mêmes souvent peu préparées sur ce sujet (avocats, huissiers, autorités, 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

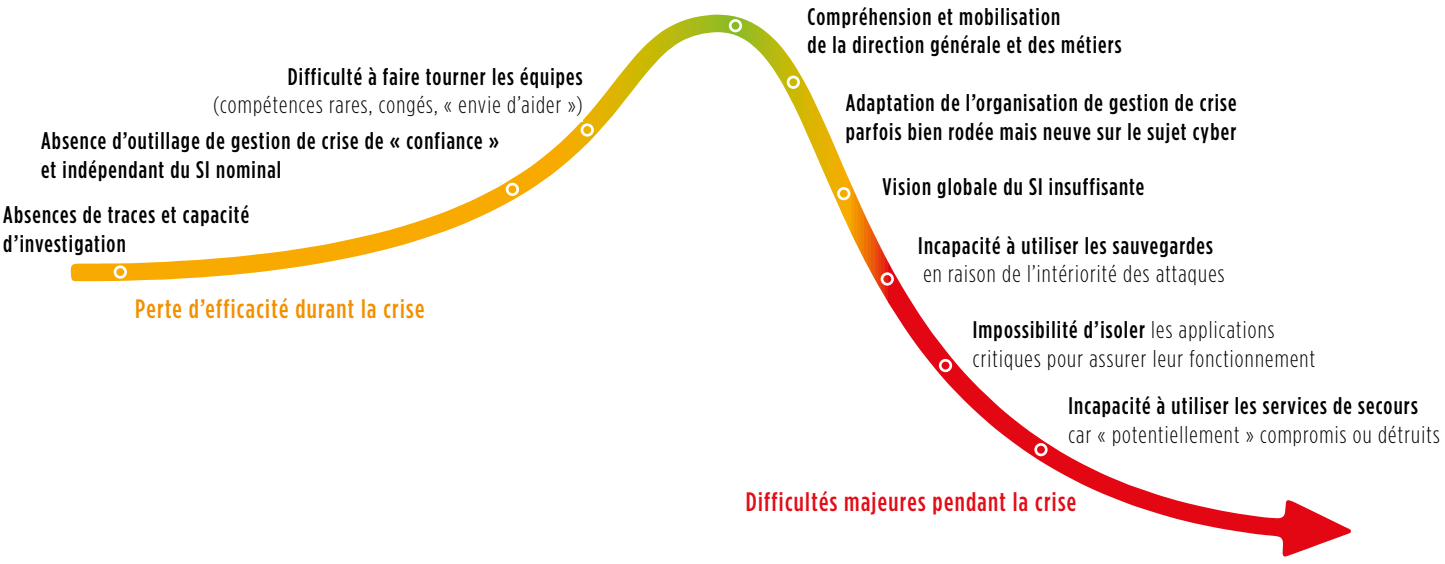
- Élévation du plafond de découvert autorisé sur un compte sans passer par le back office bancaire
- Création d'un compte administrateur AD sans création d'un ticket dans les outils de ticketing support

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.

Principaux écueils rencontrés lors de la gestion de crise cyber



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-levels 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.

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.

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...)

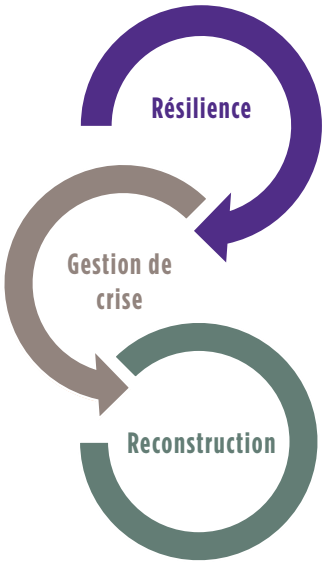
Limiter les effets d'amplification d'une attaque (durcir, cloisonner...)

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 reconstruction
(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 moyens télécoms de secours...)

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

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.