WAVESTONE

CYBER-RÉSILIENCE

PLIER POUR NE PAS ROMPRE

« Plier pour ne pas rompre », c'est souvent de cette manière que la résilience est présentée. Mais comment ce concept s'applique t-il face aux menaces cyber ? Et quelles actions réaliser pour se préparer face à des attaques de plus en plus fréquentes ?

Les cyberattaques mettent en lumière les limites de la résilience actuelle et des plans de continuité d'activité.

La continuité d'activité est souvent présentée comme un des éléments majeurs de la stratégie de résilience des organisations. Ainsi, face à des sinistres d'ampleur entraînant l'indisponibilité de ressources informatiques, d'infrastructures de communication, d'immeubles voire de collaborateurs, les organisations se sont dotées de plans de continuité d'activité (PCA) de manière à assurer leur survie.

Or les cyberattaques dans leur forme moderne, 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 la problématique de perte de confiance dans le SI induite par les cyberattaques.

De plus, les dispositifs de continuité du SI, le plus souvent liés aux ressources qu'ils protègent, sont également affectés par ces attaques. En effet, 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.

À titre d'exemple, les postes de secours dédiés et connectés des sites de repli sont aujourd'hui très souvent exposés aux mêmes risques de contamination (et destruction) que les postes nominaux.

AUTEURS

GÉRÔME BILLOIS
gerome.billois@wavestone.com

FRÉDÉRIC CHOLLET
frederic.chollet@wavestone.com

Les historiques plans de reprise/secours « à froid » (consistant souvent à activer les systèmes de secours en cas d'incident) concernent désormais de moins en moins d'applications, et il s'agit souvent d'applications secondaires.

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, du fait de l'antériorité de l'intrusion (souvent plusieurs centaines de jours avant sa détection), ces sauvegardes embarquent de fait les éléments de compromission : malwares, camps de base, mais aussi les modifications déjà opérées par les attaquants.

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.

MUSCLER LA GESTION DE CRISE

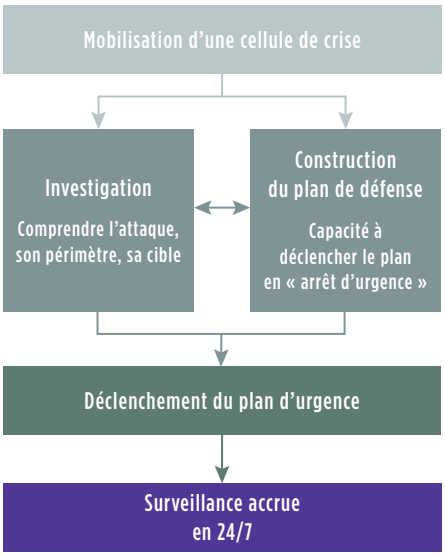
Les crises cyber sont des crises particulières : souvent longues (plusieurs semaines), parfois difficiles à cerner (qu'a pu faire l'attaquant ? depuis combien de temps ? quels sont les impacts ?) et impliquant des parties externes elles-mêmes souvent peu préparées sur ce sujet (avocats, huissier, autorités, 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. À ce titre le « Diamond Model : Graphe activity-attack » et le « Kill Chain Model » peuvent respectivement répondre à ces besoins.

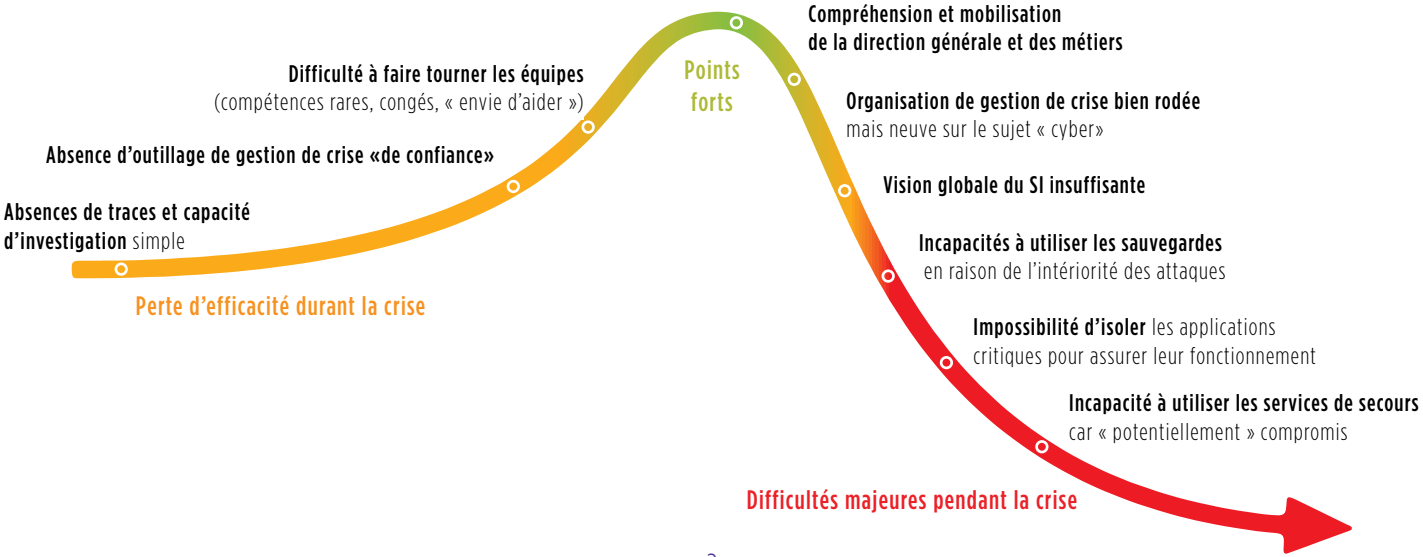
Au-delà de l'aspect organisationnel, il faudra s'assurer de disposer également de l'outillage d'investigation (cartographie, recherche de signature de l'attaque, SI de gestion de crise indépendant, capacité d'analyse de malware inconnu…) et d'assainissement (capacité de déploiement rapide de correctifs techniques, outillage de surveillance du SI…) requis pour comprendre la position prise par l'attaquant dans le SI, pour les repousser et s'assurer qu'ils ne reviennent pas.

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.

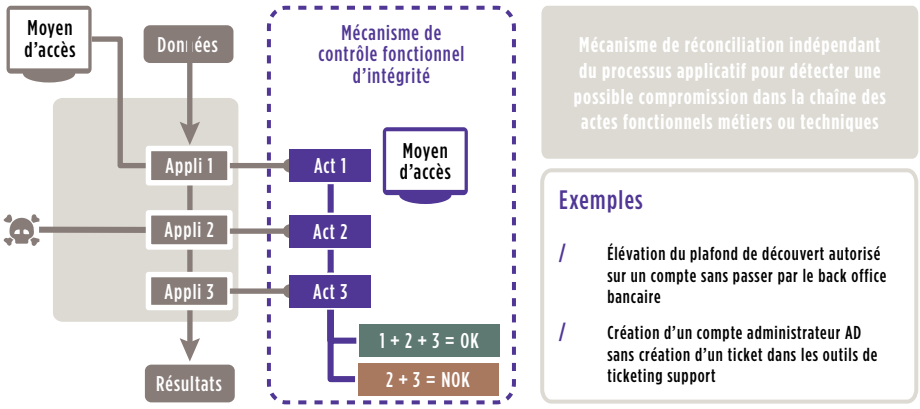
Méthodologie de gestion d'une crise cyber



Principaux écueils rencontrés lors de la gestion de crise cyber



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 évoluer pour intégrer par exemple la mise à disposition de clé 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 couteuse 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.

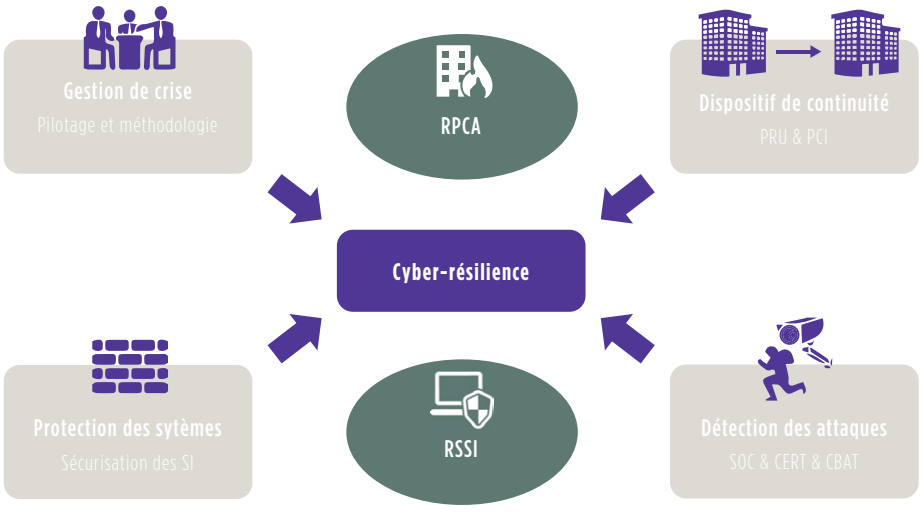
D'un niveau de complexité intermédiaire, il est possible d'envisager la définition de zone d'isolation système et réseau (« floodgate ») que l'on peut activer en cas d'attaques et qui vont isoler les systèmes les plus sensibles du reste du SI. Le SI industriel pourra, à ce titre, constituer à lui seul,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

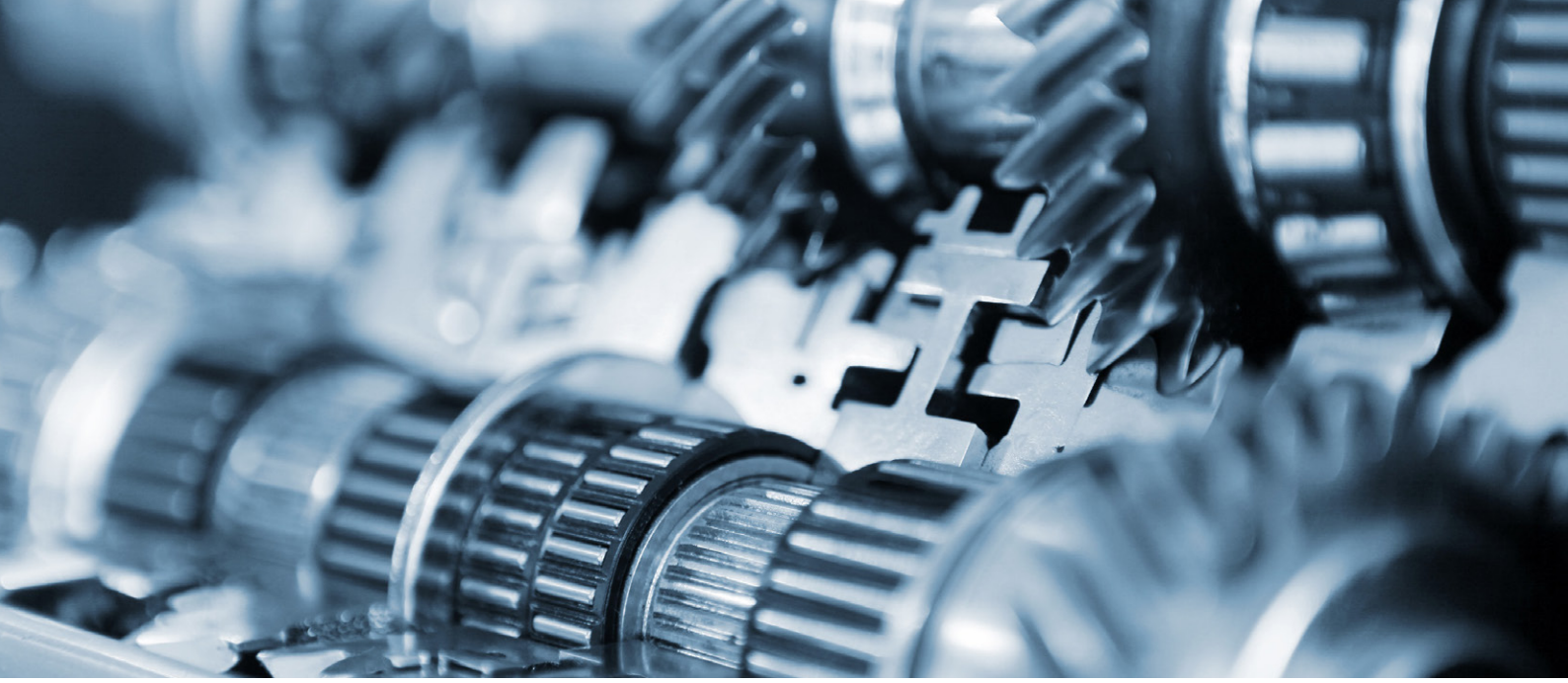
Ces évolutions, souvent majeures, doivent s'inscrire dans une revue des stratégies de secours existantes afin d'évaluer leur vulnérabilité et l'intérêt de déployer des nouvelles solutions de cyber-résilience, en particulier sur les systèmes les plus critiques. L'évolution des Business Impact Analysis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

Allier les forces du RPCA et du RSSI





SI INDUSTRIEL, SÉCURITÉ, SURETÉ ET CYBER-RÉSILIENCE : LA QUADRATURE DU CERCLE ?

Le monde industriel s'est attelé depuis de nombreuses années à concevoir des systèmes fiables face à des pannes matérielles et dont la continuité est une des composantes majeures bien ancrée dans les pratiques. Même si les cas avérés de cyberattaques sont encore peu nombreux, ils ont cependant mis en évidence la faiblesse des systèmes industriels. En particulier les mécanismes dits de « sûreté » peuvent eux aussi s'avérer inefficaces en cas d'attaques.

Parmi ces mécanismes, on peut citer les Systèmes Instrumentés de Sécurité (SIS). Ils sont censés protéger les installations et limiter les impacts en cas de défaillance. Ils ont vocation à activer des mécanismes de repli permettant de repositionner une installation dans un état stable (dérive de pression, température…) et sous contrôle. La sûreté d'une installation repose souvent essentiellement sur ces systèmes.

Or, cette confiance accordée est mise à mal par les évolutions récentes dont ont fait l'objet ces systèmes. En effet, on observe une forte tendance à la mutualisation des ressources dédiées à la conduite d'un procédé industriel avec celles visant à garantir sa sûreté. Cette mutualisation plus ou moins étendue selon les cas peut concerner les capteurs (vérification à la fois des dérives acceptables et des dérives aux limites de fonctionnement), les solveurs logiques de sûreté embarqués dans les SIS (cohabitation sur un même fond de panier d'un SIS et d'un contrôleur de procédé voire dans certain cas, fusion pure et simple du contrôleur et du SIS) ou encore le réseau véhiculant les flux de conduite et les flux de sureté sur une même liaison physique et logique. Cette mutualisation se retrouve également aux niveaux des applications de contrôle et de gestion de la sûreté fonctionnant sur une machine unique, voir sur les systèmes supports tel que les annuaires Active Directory.

Pour les responsables sécurité et sûreté des installations industrielles, la tâche s'annonce parfois encore plus complexe que pour les SI de gestion. Les évolutions devront se faire au grès des modifications apportées par les constructeurs et fournisseurs. À noter que des efforts sont constatés notamment au regard d'une règlementation qui se veut de plus en plus contraignante. Mener des premiers exercices de crise à portée cyber sur des systèmes industriels pourra constituer une première action mobilisatrice. La cyber-résilience des systèmes industriels, ne pourra être atteinte que si les sphères sécurité, continuité et sûreté travaillent ensemble.

Anthony Di Prima

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). Il figure parmi les leaders indépendants du conseil en Europe.

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.