Livre Blanc

Cinq technologies facilitant la mise en œuvre d'un framework de cyber-résilience

Sponsorisé par : IBM

Frank Dickson Phil Goodwin

Août 2019

RAPPORT MIS A JOUR

Ce document a déjà été publié en 2018 (IDC n° US44001318). Les seules modifications par rapport à la version d'origine sont le remplacement d'un des deux analystes et la nouvelle date de publication.

LE POINT DE VUE D'IDC

Une enquête récente d'IDC sur les questions de sécurité a révélé que 50 % des experts en sécurité consacraient désormais la majorité de leur temps à la sécurisation du Cloud et que, durant les 12 à 18 mois précédents, nombre d'entre eux avaient fait l'expérience de ce qu'ils décrivent eux-mêmes comme une violation liée au Cloud. Parmi les participants à cette enquête, 23 % ont indiqué qu'ils avaient été victimes d'une attaque de ransomware, 22 % ont déclaré avoir fait l'objet d'une violation IdO (Internet des objets) et 23 % d'une attaque par déni de service distribuée (ou DDoS pour Distributed Denial of Service). Environ 75 % de ces attaques ont fait suite à des incidents liés au Cloud.

Cela ne signifie pas que les technologies Cloud et les nouveaux modes de communication sont *à l'origine* de ces violations et des défaillances dans les entreprises, mais plutôt que les stratégies de protection des entreprises doivent évoluer au même rythme que l'adoption des nouvelles technologies. Ces stratégies doivent non seulement utiliser des mécanismes de sécurité renforcés et plus variés, mais aussi de méthodes de récupération rapide au cas où une violation ou un incident se produirait.

Dans le monde entier, les entreprises progressent régulièrement dans leur processus de transformation numérique, lequel consiste à intégrer la technologie à tous les aspects de l'entreprise dans le but d'accélérer les activités, de bénéficier d'une plus grande agilité, et de tirer parti d'une vision stratégique et d'opportunités dynamiques. L'un des enjeux fondamentaux de la transformation numérique consiste à devenir une entreprise structurée autour des données et capable de monétiser les informations. Simultanément, la transformation numérique s'accompagne naturellement de nouveaux risques probablement inattendus ou qui ont complexifié le profil de risque des processus bien établis dans les entreprises. En conséquence, les entreprises cherchent à élever les niveaux d'intégration entre les principales fonctions de support aux métiers et une plus grande disponibilité des données pour que l'entreprise soit prête à faire face à n'importe quel défi. Ce concept est appelé cyber-résilience.

La cyber-résilience associe les meilleures pratiques issues de la sécurité informatique, de la continuité des activités et d'autres disciplines afin de créer une stratégie en phase avec les besoins et les objectifs de l'entreprise numérique d'aujourd'hui. Ce livre blanc explique comment la transformation numérique remet complètement en question les moyens de protection traditionnels entre les entreprises et les individus participant à une économie mondiale où les technologies qui facilitent les activités ouvrent la porte aux attaques, aux risques et aux défaillances. Il explique en outre comment les pratiques de cyber-résilience peuvent aider les entreprises à se protéger contre ces risques et à reprendre leurs activités de manière contrôlée et mesurable après une violation ou une défaillance. Enfin, il fournit un cadre permettant aux entreprises de s'engager dans une logique de cyber-résilience, et décrit des stratégies visant à faire évoluer les pratiques de protection et de récupération des données afin de mieux répondre aux attaques ciblées et malveillantes d'aujourd'hui.

CE QUE VOUS TROUVEREZ DANS CE LIVRE BLANC

Peut-être qu'aujourd'hui vous connaîtrez un arrêt brutal de vos activités. Peut-être devrez-vous fermer votre entreprise aujourd'hui. Ces scénarios ne sont évidemment pas très optimistes, mais il faut savoir qu'à tout moment, certains événements perturbant la structure opérationnelle de l'entreprise sont susceptibles de se produire et, dans le monde effréné des affaires, quelle que soit l'entreprise, chaque seconde compte.

Ces événements ne doivent pas nécessairement avoir un caractère catastrophique pour avoir des conséquences durables. La plupart des entreprises expérimentées pratiquent déjà une gestion des risques et des processus permettant de mesurer la continuité et la résilience des activités. Ces entreprises ont probablement compris que les événements majeurs dont l'impact est dévastateur sont moins susceptibles de se produire que les événements discrets de moindre ampleur qui peuvent avoir des retombées opérationnelles. Considérons par exemple les craintes suscitées par la grippe aviaire. Nombreux sont ceux qui se souviennent d'une époque, au milieu des années 2000, où les entreprises se focalisaient sur l'impact potentiel d'un virus rapidement transporté dans l'air sur les employés et les activités. Bien que cette idée soit évidemment inquiétante, la probabilité qu'une menace liée à un virus aviaire ou à un autre événement similaire devienne réelle était très faible et le reste aujourd'hui. En dépit de cette faible probabilité, les entreprises ont continué à essayer de mettre en place des mesures opérationnelles de protection contre toute éventualité en fonction de la nature de l'impact potentiel. Il en va de même pour toutes les catastrophes naturelles et les menaces physiques. L'éventualité de conséquences à forts enjeux incite à réfléchir et parfois, l'attention particulière accordée à la portée potentielle d'un événement unique peut conduire les entreprises à négliger d'autres menaces, réelles, tangibles et discrètes qui peuvent avoir un impact dévastateur sur l'entreprise.

La transformation numérique bouscule la vision traditionnelle de la résilience des entreprises. La transformation numérique est un processus dans lequel la technologie est intimement liée à l'expérience humaine. Dans l'entreprise, la transformation numérique implique une très forte connectivité entre les applications et les processus métiers dans le but d'améliorer l'agilité de l'entreprise et de se connecter plus facilement aux clients et aux partenaires en visant une expérience utilisateur ininterrompue, 24h/24 et 7j/7. La transformation numérique peut prendre de nombreuses formes. Une entreprise peut chercher à améliorer l'intégration des infrastructures existantes et des systèmes traditionnels, ou à évoluer lentement vers le Cloud, ou elle peut se fixer pour mission de placer le Cloud en priorité (approche « Cloud-first »). Quoi qu'il en soit, le concept de l'entreprise connectée devient essentiel au moment d'évaluer la résilience d'une entreprise. Que cela implique de

lier les processus métiers, ou de développer des environnements multicloud ou de Cloud hybride, et dans la mesure où les systèmes et processus de l'entreprise ont tendance à devenir hyperconnectés, il existe une plus forte probabilité qu'un événement discret puisse perturber l'entreprise dans son ensemble. Ce qui n'était autrefois qu'un petit incident peut désormais déclencher des ondes de choc dans toute l'entreprise.

C'est la raison pour laquelle la cyber-résilience est devenue une préoccupation de premier plan pour les experts de la sécurité, ainsi que pour les personnes chargées d'assurer la continuité des activités et la gestion des risques. La cyber-résilience rassemble les pratiques de cyber-sécurité, de gestion des risques et de continuité/résilience des activités pour constituer une discipline axée sur l'amélioration des capacités de cyber-réponse, depuis la détection des événements et la récupération, jusqu'à l'amélioration permanente des processus. Les entreprises admettent actuellement que les stratégies traditionnelles de continuité des activités axées sur les défaillances et les pannes des systèmes ont besoin d'évoluer pour se concentrer sur les menaces informatiques malveillantes qui ciblent les données. Dans la plupart des cas, les procédures traditionnelles de reprise en cas de panne des systèmes ne seraient pas efficaces contre une cyber-menace cherchant à corrompre des données.

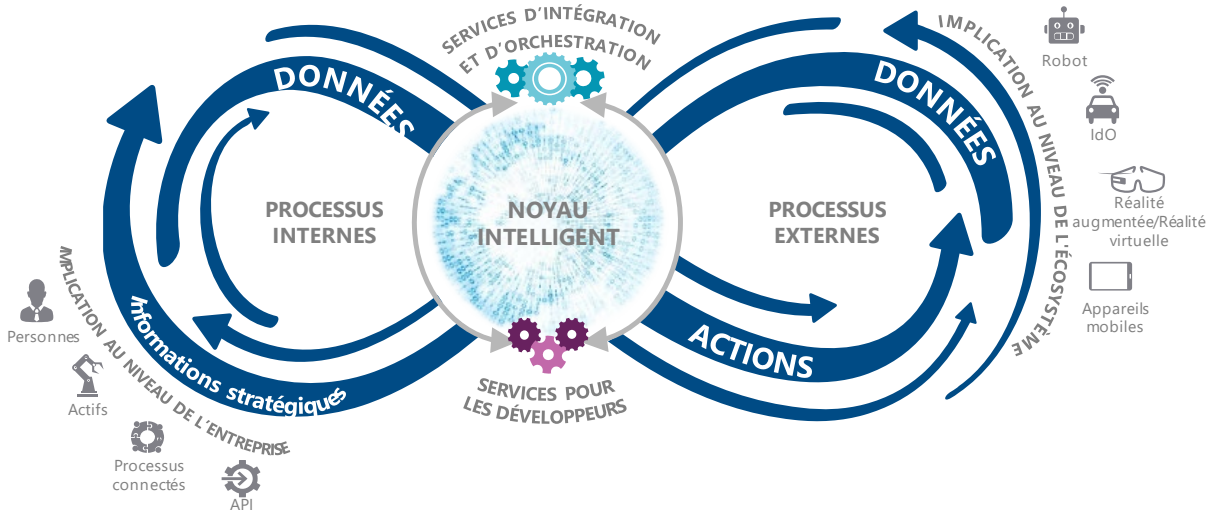
La montée en puissance et les failles de la transformation numérique

En 2017, les entreprises ont dépensé 1,1 billion $ pour essayer de se transformer en organisations connectées, intelligentes et axées sur les technologies. En 2018, ces dépenses s'élèveront à 1,32 billion $, et d'ici 2021, les entreprises du monde entier dépenseront 2,1 billions $ par an rien que dans ce but et ce chiffre continuera à augmenter. IDC pense que seulement 60 % des entreprises environ se seront engagées dans la transformation numérique d'ici 2020 et que 70 % des DSI auront défini une stratégie Cloud-first visant à améliorer l'agilité des infrastructures nécessaires à cette transformation. Il existe donc une marge de croissance considérable dans le domaine de la transformation numérique pour les trois prochaines années.

Comment expliquer un tel niveau de dépenses ? En résumé, les entreprises estiment que la transformation numérique est la voie à suivre dans un monde hyperconnecté. Elles doivent non seulement innover et faire preuve d'agilité pour survivre, mais également se préparer au lancement rapide et à grande échelle de nouveaux produits et services tout en faisant en sorte de disposer d'informations précieuses permettant d'atteindre les publics ciblés et de créer de nouveaux marchés. Concrètement, IDC estime qu'au stade ultime de la transformation numérique, la plupart des entreprises seront capables de tirer parti d'une infrastructure centrale intelligente qui utilisera des données pertinentes sur les activités de l'entreprise pour créer une intelligence exploitable et exploitée par le biais d'un processus rationalisé et ininterrompu. La plateforme de transformation numérique est le terme retenu par IDC pour décrire ce principe (voir Figure 1). Le noyau de la plateforme exploite des données diverses, distribuées et dynamiques pour créer de nombreuses opportunités.

FIGURE 1

Plateforme de transformation numérique : un cadre pour le noyau intelligent



Source : IDC, 2018

En l'absence de données, ce modèle devient bancal. Les données ne peuvent plus être produites ni monétisées. Et elles ne peuvent plus être exploitées à des fins d'agilité des activités. La survie de l'entreprise dépend donc des données dont l'intégrité et l'accessibilité revêtent dès lors un caractère sacré. Cependant, les propriétés et la localisation des données adaptées aux plateformes de transformation numérique continuent à évoluer. Les données sont de plus en plus variées. Elles ne se rapportent plus uniquement à des systèmes structurés et peuvent désormais se présenter comme des données non structurées, telles que des données de séries temporelles, des données générées par des machines et des données de diffusion. Les données deviennent également de plus en plus dynamiques. Elles ne sont plus uniquement traitées par lot et deviennent par nature des données traitées en temps réel (p. ex. les données de télémétrie sont générées à partir d'un nombre croissant de capteurs et d'appareils). En outre, les données sont de plus en plus distribuées et ne résident plus uniquement dans des datacenters centraux, mais également dans des emplacements périphériques, sur des appareils et dans des services Cloud. La nature diversifiée, dynamique et distribuée des données exacerbe le besoin de s'appuyer sur un programme efficace de cyber-résilience.

Pour autant, cela ne veut pas dire que seules les données doivent être prises en considération. Pour la plupart des entreprises, le processus de transformation numérique commence par des systèmes faiblement connectés qu'on espère pouvoir transformer en système interconnecté. Considérons la transformation numérique au regard de la machine de Rube Goldberg. Rube Goldberg était un ingénieur, un inventeur et un dessinateur lauréat du prix Pulitzer qui doit sa grande renommée à ses illustrations de systèmes complexes représentant des objets ménagers assemblés entre eux dans le but de réaliser certaines tâches banales. Cela vous rappelle quelque chose ? C'est normal. Les entreprises assemblent des systèmes de gestion des ressources humaines, de la relation clientèle, des contrats, des ERP, et bien d'autres encore, en espérant qu'ils vont converger vers un objectif commun au bénéfice de l'entreprise. C'est alors que la transformation numérique commence à

présenter des défis pour les équipes chargées de réduire les risques auxquels une entreprise est exposée.

Que se passe-t-il lorsque l'on introduit le manche d'un balai dans la roue d'un vélo ? Si les rayons de la roue ne sont reliés à rien, il ne se passera probablement pas grand-chose, mais ce n'est pas le cas. Lorsqu'un ou deux rayons sont gênés par un objet extérieur, toute la roue s'arrête de tourner. Cet exemple illustre les risques encourus par les systèmes interconnectés des entreprises. Lorsqu'un système unique tombe en panne, cela peut paralyser l'ensemble du fonctionnement de l'entreprise.

En termes de cyber-résilience, de tels liens impliquent que tout processus métier pris isolément est susceptible de constituer une passerelle vers d'autres processus métiers. Ainsi, la surface d'attaque d'un processus donné peut potentiellement autoriser un accès latéral à la quasi-totalité des autres processus.

Défis rencontrés dans le processus de transformation numérique

Bien que les dépenses consacrées à la transformation numérique soient impressionnantes, IDC constate déjà que le poids croissant des contraintes externes commence à avoir un impact important sur les stratégies de cyber-sécurité des entreprises. Comme souligné précédemment, l'interconnexion des systèmes et la dépendance permanente vis-à-vis de services externes, notamment en matière de Cloud et d'IdO (Internet des objets), s'accompagnent de risques auxquels de nombreuses entreprises ne sont pas encore préparées.

IDC estime que 60 % des entreprises environ se seront engagées dans la transformation numérique d'ici 2020 et que 70 % des DSI auront défini une stratégie Cloud-first. Bien que ces chiffres soient frappants, il n'existe pas d'information claire sur le nombre d'entreprises conscientes que la disponibilité des données et des applications (informations) est essentielle à la réussite de la transformation numérique. Si les données ne sont pas disponibles, elles ne peuvent pas être monétisées. Une plus grande disponibilité des données procure aux entreprises un avantage sur les concurrents moins avancés dans ce domaine. Même si IDC a constaté une augmentation des dépenses dans les produits et services anti-DDoS, de nombreuses entreprises ont du mal à progresser dans la définition d'une stratégie cohérente de disponibilité des informations permettant de préserver rapidement et de bout en bout la disponibilité des données/informations dans tout le processus d'accès aux données.

Le renforcement de la conformité réglementaire constitue un autre défi issu de l'extérieur de l'entreprise. D'ici 2025, plus de 70 % des données d'entreprise devront répondre à des contraintes de conformité réglementaire. Non seulement ces données nécessitent un traitement particulier, mais elles sont également à l'origine de risques supplémentaires pour les entreprises qui pourraient être lourdement pénalisées en cas de défaut de protection de ces données.

La dépendance croissante à l'égard du Cloud et de l'IdO

La disponibilité des données et la conformité sont des contraintes externes ayant un impact important sur l'entreprise, mais sur lesquelles celle-ci n'a parfois qu'une influence indirecte. Ce constat est d'autant plus éloquent si l'on considère que de plus en plus d'entreprises sont dépendantes du Cloud et de l'IdO (Internet des objets) pour les fonctions métiers critiques.

Aujourd'hui, les entreprises utilisent le Cloud hybride et la plupart des prochaines applications s'appuieront sur le Cloud. Au cours d'une enquête récente, les entreprises ont rapporté que la moitié de leurs applications sont actuellement déployées sur la base d'un modèle de Cloud hybride. Les répondants du même groupe prévoient que 62 % de leurs applications fonctionneront sur un Cloud hybride d'ici les deux prochaines années. Les considérations de sécurité représentent à la fois un moteur et un frein pour l'adoption du Cloud hybride. Les données critiques sont désormais réparties entre de nombreux emplacements, datacenters et environnements Cloud. Ces données doivent être protégées conformément aux exigences de l'entreprise, quel que soit l'endroit où elles résident. Les entreprises interrogées s'attendent à ce que les dépenses consacrées aux services de données pour le Cloud hybride augmentent de 40 % au cours des 12 prochains mois. Les sauvegardes, les récupérations, la détermination des coûts des données et l'estimation de leur valeur figurent parmi les principales priorités.

Les entreprises collectent de plus en plus de données sensibles non seulement à partir du Cloud, mais également via l'IdO. Bien que ces dispositifs disposent d'une puissance de traitement inférieure à celle de systèmes complets, les pirates ont démontré qu'ils étaient capables de les exploiter dans le cadre d'une stratégie d'attaque. Cette capacité associée à des carences générales en matière de sécurité des dispositifs IdO impose aux entreprises d'identifier le meilleur moyen de protéger ces appareils susceptibles de poser des difficultés d'accès, de surveillance et de sécurisation tout en continuant à assurer la protection du matériel informatique traditionnel.

Des pannes de plus en plus complexes

Bien qu'IDC ait pu constater que les entreprises se montraient plus confiantes dans leur capacité à sécuriser le Cloud et que les taux de migration vers le Cloud, ainsi que l'adoption de solutions de sécurité basées sur le Cloud, se soient renforcés, les entreprises n'ont jamais semblé aussi mal préparées face au défi de la complexité croissante des pannes.

Au cours d'une enquête récente conduite par IDC auprès d'entreprises, 56 % des répondants ont mentionné avoir fait l'objet d'une attaque par déni de service de type DDoS ayant duré entre 5 et 24 heures. D'autres répondants (8 %) ont fait part d'une attaque ayant duré entre 1 et 7 jours et, encore plus alarmant, 6 % des répondants avaient fait l'objet d'une attaque d'une durée dépassant 8 jours.

Les sauvegardes et les reprises après sinistre ne suffisent pas à assurer une protection contre les attaques modernes. Les meilleures pratiques recommandées par IDC font état d'une durée maximale d'interruption admissible (RTO – Recovery Point Objective) d'une heure pour les applications critiques et de quatre heures pour les autres applications. Certaines copies définies dans le temps (snapshot) peuvent être incomplètes, inefficaces et vulnérables aux attaques si elles n'ont pas été conçues de manière appropriée. Dans de nombreux cas, l'approche retenue consiste à prévoir une récupération au niveau du système et non de l'environnement, comme cela serait nécessaire en cas de corruption d'une plateforme ou d'une configuration. Une maintenance et des tests insuffisants sont également susceptibles d'annihiler des schémas solides de protection des copies de données définies dans le temps.

Les travaux d'IDC indiquent que le coût « moyen » des temps d'arrêt dépasse 200 000 $ par heure, bien que ce chiffre varie en fonction de la taille de l'entreprise et du secteur dans lequel elle évolue. En général, il sera possible de s'appuyer sur ce coût pour aider l'entreprise à orienter ses choix en matière de conception de plans de résolution et d'infrastructure. L'estimation des coûts tient compte des pertes réelles de chiffre d'affaires et des coûts de récupération (dont les coûts liés à la réglementation) qui peuvent être élevés. En revanche, ils ne tiennent pas compte des coûts liés à l'impact sur la réputation de l'entreprise et sur la dégradation de l'image de marque à long terme qui peuvent découler d'une violation embarrassante. Toutefois, ces estimations de coûts peuvent être utilisées pour contribuer à déterminer les dépenses pertinentes pour une entreprises pour la mise en place d'une stratégie pertinente. L'exemple d'une apparition récente d'un ransomware illustre ce propos. La ville d'Atlanta a récemment dépensé presque 3 millions $ dans un plan d'urgence au cours des trois semaines qui ont suivi un incident lié à un ransomware ayant entraîné une indisponibilité de certains services municipaux. Il a été rapporté que la ville avait demandé un budget supplémentaire de 9,5 millions $ pour financer la reprise des activités et renforcer les mesures de protection. À première vue, ce montant de financement supplémentaire peut paraître extrêmement élevé. Mais si vous prévoyez d'éviter de devoir à nouveau dépenser 3 millions $ dans des mesures anti-ransomware dans un avenir prévisible, la somme de 9,5 millions $ dépensée en une fois pour renforcer les niveaux de protection semble bien plus raisonnable.

L'essor des attaques évoluées

IDC continue de constater une augmentation du nombre des attaques complexes. Les études statistiques indiquent que de nombreuses attaques ne sont pas détectées avant 200 jours. En disposant d'une période aussi longue pour évoluer en secret dans un réseau, les pirates peuvent implanter des logiciels malveillants capables de s'infiltrer dans des configurations de sauvegarde, infectant par la même occasion les données de récupération. Les attaques peuvent demeurer latentes pendant des semaines ou des mois, et permettre ainsi à des logiciels malveillants de se propager dans tout le système. Même lorsque l'attaque a été détectée, il peut être extrêmement difficile de supprimer le logiciel malveillant compte tenu de sa large propagation dans l'entreprise.

VUE D'ENSEMBLE DE LA SITUATION

Le concept de cyber-résilience

Les ressources d'infrastructure sont de plus en plus disponibles dans le Cloud et via l'Internet des Objets. Cependant, les moyens de protection traditionnels visant à contrer les nouvelles menaces se montrent inefficaces. En conséquence, les entreprises doivent adopter une nouvelle approche. Les types de menaces qui sévissent aujourd'hui exigent de faire appel à une solution intégrée efficace durant tout le cycle de vie des données. Les entreprises doivent s'attacher à réduire la durée entre les étapes de protection, détection, réponse et reprise durant le cycle de vie lors de la mise en place des capacités de cyber-résilience.

Le framework de la cyber-résilience

La cyber-résilience est un framework conçu pour aider les entreprises à résister aux attaques. Elle ne consiste pas en une couche de protection ou un produit unique, mais constitue plutôt un moyen permettant aux entreprises de structurer leur protection de telle sorte qu'aucun événement ne puisse avoir de conséquences catastrophiques. La cyber-résilience est un processus itératif fournissant des moyens de récupération après une attaque. Par rapport aux systèmes de protection traditionnels qui

ne servent plus à rien dès lors qu'ils ont été contournés, la cyber-résilience permet de garantir une vigilance constante dans toute l'entreprise.

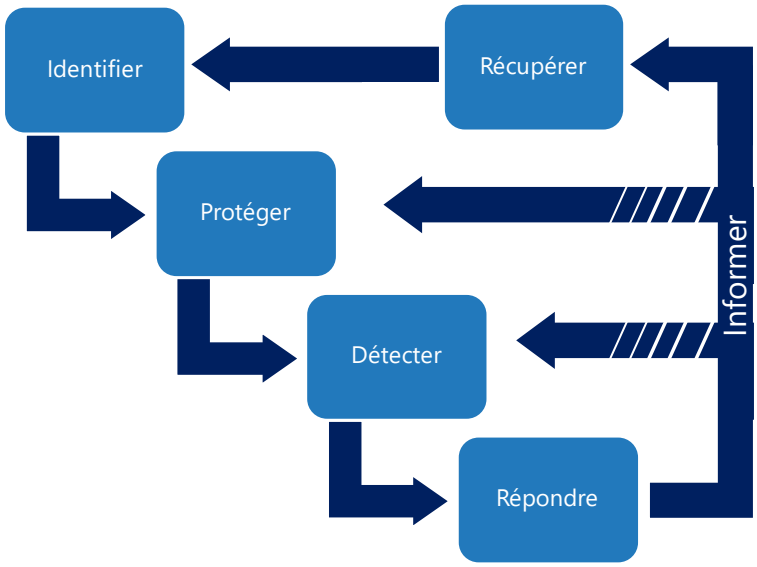
Le framework de la cyber-résilience est composé des cinq actions suivantes (voir Figure 2) :

- **Identifier :** Cartographier les actifs et processus critiques, évaluer les risques et le niveau de préparation de l'entreprise, etc.
- **Protéger :** Actionner les mécanismes de sécurité traditionnels assurant une première ligne de protection
- **Détecter :** Effectuer une analyse de sécurité
- **Répondre :** Remédier aux violations et failles de sécurité
- **Récupérer :** Actionner les mécanismes coordonnés de récupération

Le principal avantage de ce framework de la cyber-résilience réside dans sa capacité à faire progresser l'entreprise. Traditionnellement, la sécurité était une couche placée au-dessus de l'entreprise. La cyber-résilience intègre la sécurité au cœur de l'entreprise, permettant à ces cinq composantes d'être présentes dans tous les domaines de l'entreprise.

FIGURE 2

Le framework de la cyber-résilience



Source : IDC, 2018

L'incident par opposition aux conséquences

Il a été démontré à maintes reprises que les attaques iront jusqu'au bout de la mission pour laquelle elles ont été conçues. La sécurité est une discipline complexe, et il n'existe tout simplement aucun moyen de prouver qu'un environnement est sûr. Les pirates trouvent toujours des méthodes innovantes pour s'introduire dans une entreprise en ayant recours à toutes les tactiques permettant de lancer une attaque qui atteindra son objectif. Au mieux, une entreprise peut espérer pouvoir s'appuyer

sur une infrastructure renforcée, des fonctions et des processus auditables, des utilisateurs parfaitement formés, une équipe de sécurité ultra-compétente et des processus de surveillance ininterrompue. Une telle configuration serait idéale, mais pour la plupart des entreprises, la solution peut consister à réfléchir d'une manière différente sur ce qui se passe après une attaque. Si l'on sait déjà qu'une attaque ira jusqu'au bout de sa mission quels que soient les contrôles et mesures de vérification et de compensation mis en place, ne serait-il pas logique de se préparer à faire face aux conséquences plutôt qu'à l'incident en tant que tel ? Lorsqu'une attaque réussit, les entreprises doivent trouver un moyen de réduire la durée entre la détection et la réponse, ainsi qu'entre la réponse et la reprise. Plus une entreprise sera capable d'assurer la continuité des opérations, même à la suite d'une cyber-attaque réussie, mieux elle se portera.

Une entreprise ne peut se permettre la moindre interruption de ses activités. Peu importe le niveau de sophistication d'une attaque ou la façon dont le pirate a pu s'infiltrer dans l'entreprise, l'entreprise doit continuer à fonctionner. En tirant profit des stratégies de réduction des délais opérationnels de détection, de réponse et de reprise, les entreprises ne se limitent pas à diminuer les coûts découlant d'un incident, elles se créent finalement un avantage concurrentiel. IDC pense que les entreprises capables de minimiser les perturbations bénéficient d'un avantage important sur les entreprises mal préparées en créant un climat de confiance avec les consommateurs et les partenaires commerciaux.

PERSPECTIVES D'AVENIR

Les cinq technologies clés de la cyber-résilience

Bien que le framework de la cyber-résilience puisse sembler naturel au premier abord, il doit être mis en œuvre à l'aide de technologies soigneusement choisies. Il n'existe pas de produit unique capable de créer un environnement cyber-résilient, mais il existe des technologies qui peuvent être mises en œuvre pour parer aux éventuelles perturbations des activités en cas de cyber-attaque. Les cinq technologies présentées dans les sections suivantes sont essentielles à la création d'un environnement résilient.

Automatisation et orchestration pour la récupération des plateformes et des données applicatives

Le terme *automatisation* a longtemps effrayé les experts de la sécurité. Les préoccupations liées à l'automatisation perdurent dans toute l'industrie depuis que les solutions automatisées existent. Cependant, compte tenu des attaques actuelles largement automatisées, une automatisation intelligente est essentielle. mais au lieu de considérer l'automatisation comme la solution, l'orchestration et l'automatisation doivent faire partie de la réponse.

L'orchestration ne consiste pas à écarter la variable humaine de l'équation ou à permettre des changements de politique aveugles, mais plutôt à donner plus de moyens aux analystes en leur fournissant un accès rapide à des informations, ainsi que la capacité d'apporter une réponse plus rapidement qu'avec des méthodes manuelles. En outre, une reprise réussie des applications nécessite de récupérer en plusieurs étapes les systèmes et données interconnectés. La récupération manuelle de ces systèmes peut introduire des erreurs humaines, tandis que l'automatisation des processus de récupération à l'aide de modèles logiciels validés et testés peut atténuer les risques au cours du processus de récupération.

Protection Air Gap (par isolation physique) pour des sauvegardes sécurisées visant à lutter contre les logiciels malveillants propagés

La technique de l'Air Gap consiste à séparer physiquement ou virtuellement un système ou un réseau des autres systèmes ou réseaux. Par exemple, les entreprises peuvent faire en sorte que les réseaux ou les systèmes contenant des données extrêmement sensibles soient complètement séparés du réseau gérant les opérations quotidiennes.

Bien que la notion de périmètre ait disparu et que les entreprises souhaitent que leurs données circulent de manière fluide dans toute l'organisation, la capacité à créer des segments isolés du réseau n'a jamais revêtu une telle importance. Comme nous avons pu le constater avec les attaques récentes par ransomware, une partie automatisée d'un logiciel malveillant peut avoir été conçu pour traverser rapidement le réseau et faire des ravages en très peu de temps. L'entreprise est ainsi exposée en interne et potentiellement vis-à-vis de l'extérieur selon le ou les systèmes affectés. Aujourd'hui, la meilleure pratique consiste à créer une copie en air gap des données critiques afin d'atténuer cette exposition extérieure, de protéger l'entreprise des temps d'arrêt opérationnel et d'éviter les coûts injustifiés.

La technique Write Once, Read Many/stockage non effaçable pour empêcher la corruption ou la suppression des données

Les attaques récentes de ransomware, telles que NotPetya, ont mis en évidence le besoin d'une meilleure protection contre la corruption et la suppression de données. Nous savons que les pirates cherchent à effacer les journaux (logs) pour supprimer toute trace de leurs activités, mais la suppression ou la corruption des données peut anéantir une entreprise. Après l'apparition de WannaCry et autres ransomware récents, beaucoup d'entreprises ont constaté que le paiement de la rançon ne permettait pas toujours d'obtenir la clé de chiffrement de la part des pirates. Dans certains cas, la clé fournie par le pirate n'a même pas fonctionné.

Les entreprises doivent disposer de technologies permettant de créer des données inaltérables. La technique Write Once, Read Many (WORM)/stockage non effaçable peut répondre à ce besoin. Grâce à ce type de technologie, une entreprise peut préserver l'intégrité de ses données et assurer la résilience de ses activités face à des attaques qui ont été parmi les plus dévastatrices de ces derniers temps. Il existe plusieurs formes de technologies WORM au niveau de la couche logicielle et de la couche matérielle. Ces deux méthodes constituent un moyen de veiller à ce que les données ne soient pas altérées et fournissent une chaîne de traçabilité électronique.

L'efficacité des copies définies dans le temps et de la vérification des données pour l'identification rapide des données récupérables

Après une attaque, les entreprises doivent disposer d'un moyen leur permettant de valider et de restaurer rapidement une copie « saine » de leurs données. Comme souligné précédemment, beaucoup de pirates peuvent évoluer dans les systèmes pendant des mois, ce qui signifie souvent que les sauvegardes sont également infectées. Cela oblige à faire appel à des technologies efficaces de copies définies dans le temps pour conserver de multiples copies des données. Une vérification permanente des données présentes sur ces copies est nécessaire afin de pouvoir identifier les infections éventuelles de manière proactive et de prendre des mesures correctives. Cette vérification permet également d'identifier la copie saine qui sera utilisée au cours du processus de récupération. Il existe différentes méthodes de vérification des données sauvegardées qui s'appuient sur des caractéristiques matérielles et logicielles, et permettent de garantir que les données n'ont pas été infectées.

La vérification des données s'impose pour les processus de test des reprises après sinistre et opérationnelles. Tout d'abord, il sera nécessaire de s'assurer de l'intégrité des données sauvegardées/répliquées et que le processus de sauvegarde/réplication s'est déroulé comme prévu. Ensuite, il faudra inspecter ces données sauvegardées/répliquées pour s'assurer que l'infection qui a touché les données en production ne s'est pas propagée aux données sauvegardées/répliquées. En fonction du système sauvegardé, les utilisateurs souhaiteront éventuellement utiliser des techniques différentes de vérification des données. Par exemple, un système de base de données peut disposer d'un outil de triage et d'inspection qui viendra compléter de manière pertinente les fonctionnalités offertes par une solution plus globale de protection des données.

Rapports réglementaires et assurances

Bien que la conformité réglementaire soit souvent considérée comme une contrainte obligatoire ne permettant pas d'améliorer la sécurité d'une entreprise dans son ensemble, il convient de reconnaître que valider la présence de contrôles appropriés, ainsi que leur bon fonctionnement peut se révéler extrêmement efficace. En outre, compte tenu de l'augmentation du montant des amendes pour non-conformité, un reporting efficace peut aider les entreprises à démontrer qu'elles respectent la réglementation, et leur permettre d'économiser du temps et de l'argent par rapport aux coûts des audits et amendes potentielles.

DEFIS ET OPPORTUNITES

Dans l'environnement actuel des entreprises, la cyber-sécurité est le principal défi à surmonter. Le rythme et le volume des menaces de sécurité représentent des défis auxquels les entreprises, quelle que soit leur taille, doivent se mesurer pour conserver une longueur d'avance. Il convient donc d'accorder encore plus d'importance à la planification et au déploiement de stratégies de cyber-résilience. Une stratégie de cyber-résilience efficace doit avoir une large portée et faire appel à de nombreux intervenants, pas seulement des experts du domaine de la sécurité, des opérations, de l'ingénierie, du droit et du risque, mais également les Data Owners (propriétaires des données) et les responsables fonctionnels. Une collaboration et une planification entre tous ces groupes, dont les priorités et la portée des connaissances diffèrent, sont donc nécessaires. Cette dynamique organisationnelle représente un défi dans la plupart des grandes entreprises, lequel peut cependant être surmonté grâce à une planification stratégique et une définition des priorités au niveau de la direction.

CONCLUSION

La cyber-résilience joue un rôle essentiel dans la disponibilité des données et des applications. Elle est également une composante clé du processus de transformation numérique. Sans une cyber-résilience appropriée, les entreprises seront de plus en plus vulnérables aux attaques susceptibles de paralyser leur fonctionnement. Outre les attaques malveillantes, le nombre croissant de réglementations applicables dans différentes zones géographiques et différents secteurs expose les entreprises à des risques d'amendes importantes en cas d'absence ou de défaut des processus de validation des contrôles.

Cette pratique ne se limite pas à la détection des logiciels malveillants, aux sauvegardes ou aux reprises après sinistre. Elle consiste en une approche intégrée du cycle de vie visant à assurer la disponibilité des données, quelles que soient les menaces, et qui englobe la plateforme. La cyber-

résilience doit à la fois tenir compte des référentiels de données sur site et de ceux situés dans le Cloud. Les services informatiques doivent opter pour une approche complète de la cyber-résilience et rechercher des produits et solutions qui permettent de répondre à l'ampleur des cybermenaces.

En définitive, la cyber-résilience est un framework avec des moyens pour récupérer après une attaque. Cependant, il est nécessaire de disposer d'un ensemble pertinent de technologies sous-jacentes afin de s'assurer que chaque étape de ce framework puisse être traitée. La sécurité ne peut plus être définie en termes de niveaux variables de confidentialité, d'intégrité et d'accessibilité ; elle doit systématiquement englober les trois piliers. Les entreprises qui mettent en œuvre la cyber-résilience bénéficient d'un avantage concurrentiel quand les clients sont confrontés ailleurs à des problèmes de disponibilité. Une entreprise résiliente est capable de s'adapter aux attaques et de se relever.

À propos d'IDC

International Data Corporation (IDC) est le premier fournisseur mondial d'informations commerciales stratégiques, de services-conseils et d'événements d'informatique, de télécommunications et de produits technologiques grand public. IDC aide les professionnels de l'informatique, les dirigeants d'entreprise et la communauté des investisseurs à prendre des décisions qui se fondent sur des faits pour les achats technologiques et la stratégie de l'entreprise. Plus de 1 100 analystes d'IDC apportent une expertise mondiale, régionale et locale sur diverses opportunités technologiques et sectorielles, ainsi que sur les tendances qui se dégagent dans plus de 110 pays à travers le monde. Depuis 50 ans, IDC offre des informations stratégiques et détaillées permettant à ses clients d'atteindre leurs objectifs commerciaux clés. IDC est une filiale d'IDG, une des principales sociétés en matière de médias, de recherche et d'événements liés à la technologie.

Siège social mondial :

5 Speen Street

Framingham, MA 01701

États-Unis

+1.508.872.8200

Twitter: @IDC

idc-community.com

www.idc.com