Livre Blanc

Protection des données, remédiation, gouvernance : l'évolution de la sécurité informatique au sein des grands comptes en France

Sponsorisé par : IBM

Karim Bahloul
Juin 2017

INTRODUCTION

Les failles de sécurité sont aujourd'hui inévitables. Leur sophistication ne cesse de croître. La question n'est plus tant de savoir comment arrêter définitivement ces attaques mais plutôt d'identifier les leviers qui permettront de réduire et maîtriser leurs impacts sur l'activité de l'organisation. Chaque nouvel incident de sécurité est l'occasion pour les RSSI (Responsable de la Sécurité des Systèmes d'Information) de sensibiliser un peu plus la Direction Générale de l'entreprise sur les risques encourus et sur la nécessité de renforcer les politiques de sécurité. La dernière attaque "médiatique" en date – Wannacry – a même inversé la donne : de nombreuses Directions Générales ou Directions métiers ont devancé leurs équipes de sécurité en leur demandant d'évaluer rapidement le niveau d'exposition de l'entreprise aux risques.

Au-delà des menaces immédiates et spectaculaires, la prise de conscience de la Direction Générale est alimentée par deux phénomènes d'envergure : le Règlement Général sur la Protection des Données (voté mi 2016 et applicable à partir de mai 2018) et le mouvement généralisé des grandes entreprises vers une transformation numérique en profondeur de leurs processus métiers et de leur modèle économique. En d'autres termes, l'impact d'une faille de sécurité, qui mettrait en danger les données personnelles, devient pour l'entreprise un risque majeur : ce risque est désormais encadré par une loi (le GDPR) qui prévoit des pénalités importantes en cas de non-respect. Par ailleurs, la transformation numérique diffuse cette notion de risque à tous les niveaux de l'entreprise et à tous ses départements : l'exposition aux risques s'en trouve décuplée.

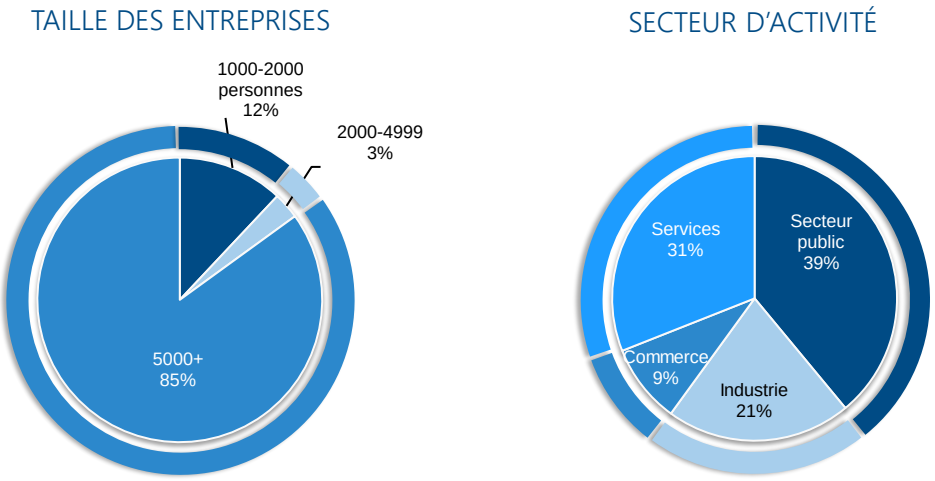
De nombreuses questions se posent alors pour les entreprises : comment protéger les données portant sur les salariés, les clients, les produits et services, les partenaires, la stratégie de l'organisation ou encore sa politique d'innovation, sans entraver le business ? Comment renforcer l'efficacité des politiques de sécurité dans un environnement contraint par les coûts et par le manque d'effectif ? Quels choix faire en matière d'externalisation ? Comment assurer une gouvernance optimale qui permette de définir le bon équilibre entre processus, compétences et technologie ?

METHODOLOGIE

Pour réaliser cette étude, IDC a interrogé au cours du 1er semestre 2017, 33 organisations de grande taille basées en France, dans tous les secteurs d'activité dont les services financiers, la distribution, l'industrie, la santé, les services, le secteur public, les télécommunications et les médias. La plus grande part des structures interrogées dispose de plus de 5 000 salariés sur la France, les autres appartiennent au SBF120. Les fonctions interrogées sont des responsables de la sécurité des systèmes d'information. Afin de permettre une exploitation dans le cadre de cet observatoire et une représentativité du marché, les résultats ont été redressés conformément aux statistiques de l'INSEE.

GRAPHIQUE 1

Méthodologie de l'étude : Typologie des entreprises interrogées



Source: IDC, 2017

LES PRIORITES INFORMATIQUES DES ENTREPRISES ET LEURS IMPACTS SUR LA POLITIQUE DE SECURITE : 3 NIVEAUX DE MATURITE

La politique de sécurité des systèmes d'information, même si elle est une priorité forte dans l'agenda des entreprises, est souvent en décalage avec les initiatives informatiques que projettent les entreprises. Les deux sujets ne progressent pas au même rythme, l'une (la politique de sécurité) prenant le plus souvent le relais de l'autre (les projets métiers).

- C'est le cas par exemple des initiatives de transformation numérique. Elles sont la priorité majeure des entreprises pour les prochains mois (selon 83% des structures interrogées), mais toutes ces entreprises n'ont pas encore pleinement anticipé l'impact de cette transformation sur leur politique de sécurité (uniquement 64% pour lesquelles les impacts sur la politique de sécurité seront importants). Selon IDC, les entreprises devront prendre rapidement conscience que la diffusion massive des projets de transformation numérique dans l'entreprise aura des impacts majeurs sur leur politique de sécurité. C'est à cette condition que les initiatives de sécurité IT pourront être pleinement alignées avec les

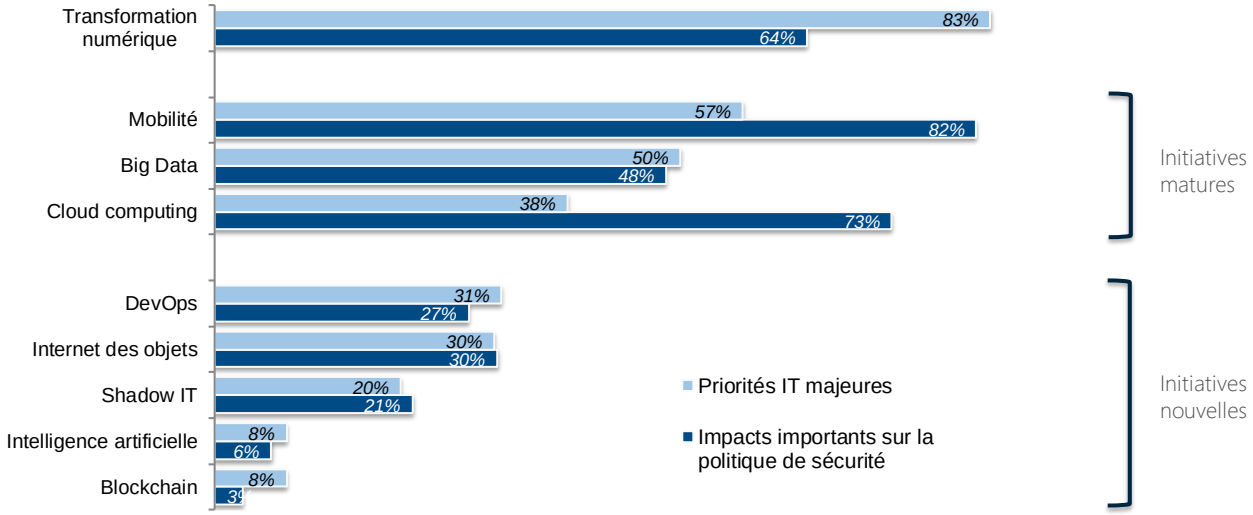
enjeux d'une telle transformation (ouverture des systèmes d'information, développement des micro-services, multiplication des accès clients et partenaires aux données du système d'information);

- Inversement, les sujets plutôt matures tels que le Cloud Computing et la mobilité, sujets sur lesquels les entreprises ont beaucoup investi au cours des 3 dernières années, deviennent logiquement moins prioritaires pour les 18 prochains mois. Mais face à la diffusion massive de ces technologies dans l'entreprise, les directions informatiques et celles en charge de la sécurité prennent conscience de leurs impacts majeurs sur leur politique de sécurité. Ainsi, 82% des directions informatiques constatent que les efforts en matière de sécurisation des environnements mobiles devront être importants pour faire face à la démocratisation des initiatives de mobilité. Il en est de même pour le Cloud Computing. Ce sujet est prioritaire pour seulement 38% des grandes structures interrogées dont un grand nombre a lancé ce type d'initiative depuis plusieurs années. Néanmoins, 3/4 d'entre elles constatent que les impacts sur leur politique de sécurité (et sur les investissements associés) sont importants.

- Enfin, les sujets sur lesquels les entreprises investissent en avance de phase (Blockchain, Intelligence Artificielle, Internet des Objets, DevOps) ne sont pas considérés par les entreprises comme des initiatives qui impacteront de manière significative leur politique de sécurité. C'est pourtant à ce stade initial de réflexion que les entreprises devraient anticiper les impacts que pourront avoir ces technologies novatrices sur la sécurité du SI.

GRAPHIQUE 2

Quelle adéquation entre les priorités informatiques et les impacts des différentes initiatives sur la politique de sécurité ?



Source: IDC, 2017

Selon IDC, les entreprises devront rapidement réaligner leur politique de sécurité sur les initiatives informatiques qu'elles mènent ou qu'elles projettent de mener. D'autant plus que c'est une prérogative du règlement européen sur la protection des données (GDPR). En effet, le "privacy by design" et le "security by design" sont des notions qui imposent désormais aux entreprises d'intégrer, dès la conception des projets applicatifs et des projets d'infrastructure, la protection des données personnelles et leur sécurisation.

SECURITE INFORMATIQUE : VERS UNE NOUVELLE DYNAMIQUE INSUFFLEE PAR LE GDPR

La nécessité de répondre aux exigences réglementaires imposées par le règlement européen sur la protection des données (GDPR) devient prioritaire au sein des grands comptes en France. Le GDPR est d'ailleurs considéré par nombre d'entreprises comme une opportunité de réaligner les priorités technologiques et les enjeux de sécurité pour que les deux sujets évoluent au même rythme.

Les entreprises rencontrées par IDC dans le cadre de cette étude témoignent de cet état de fait. Ainsi, le RSSI d'une grande enseigne de la Banque indique que "***le responsable de la sécurité des systèmes d'information était jusqu'alors considéré comme l'interlocuteur qui empêchait les directions métiers d'avancer sur des projets métiers déjà initiés et souvent prioritaires. Avec le GDPR, la donne change progressivement : le RSSI doit être intégré dès le lancement du projet pour assurer le respect des exigences réglementaires en matière de protection des données personnelles. Etant donnés les enjeux business et financiers (pénalités en cas de non-respect, risques sur la réputation de l'entreprise), l'implication du RSSI ne sera plus vécue comme une contrainte ou un frein mais comme une nécessité pour l'entreprise et les directions métiers".***

Qu'est-ce que le GDPR ?

Le GDPR (General Data Protection Regulation) a été mis en place par l'Union Européenne pour unifier la réglementation en direction des entreprises qui traitent, stockent ou collectent des données. Il représente le plus grand bouleversement de ces dernières années dans le domaine juridique de la protection et de la confidentialité des données. Les entreprises doivent se mettre en accord avec le règlement européen et son lot de nouvelles exigences en matière de protection des données personnelles d'ici mai 2018. Le GDPR a pour objectif de faire face à l'internationalisation du marché autour des données personnelles, et harmoniser la politique liée à ces données entre les différents pays européens. Il concerne toutes les entreprises européennes ou non, qui détiennent des données sur des citoyens européens.

Quelles sont les dispositions prévues par le GDPR ?

Ce nouveau règlement, qui s'applique à tous les secteurs d'activités, et pour les organisations de tout type et de toutes tailles, impacte la gestion des données personnelles sur de nombreux aspects dont :

- Une protection accrue des données personnelles en termes de consentement, d'accessibilité et de portabilité.
- Les clients et utilisateurs des données des entreprises ont le droit de demander l'effacement de leurs données, la rectification ou la récupération de celles-ci dans un format clair et réutilisable.
- L'intégration des exigences de respect de la vie privée dès la conception des systèmes de traitement de données personnelles.
- Une simplification des formalités administratives pour les entreprises (avec la création d'un guichet unique).
- Une obligation pour les entreprises de démontrer la bonne application du règlement.
- L'exigence d'un représentant dans l'union.
- La désignation d'un DPO (Délégué à la Protection des Données) au sein des entreprises, qu'il soit interne ou externe.

- La notification des failles de sécurité dans les 72 heures.
- La mise en place d'un registre des traitements obligatoire pour les entreprises de plus de 250 salariés (ou pour les entreprises de moins de 250 salariés pour lesquelles le traitement des données est au cœur leur activité).
- Une sanction à hauteur de 4% de leur chiffre d'affaires mondial ou 20 Millions € pour les entreprises qui ne respecteront pas les exigences du GDPR.

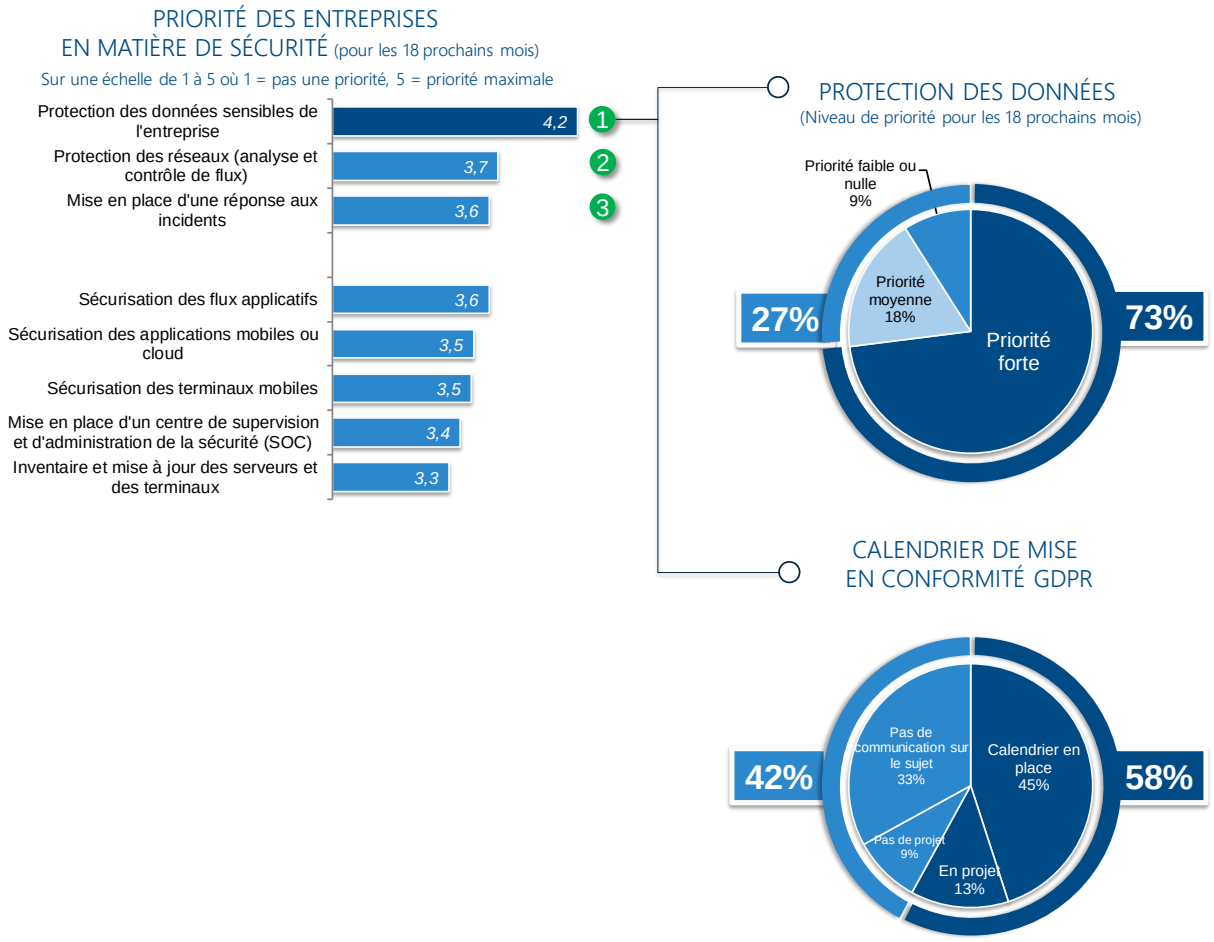
La protection des données, au 1er rang des priorités de sécurité pour les 18 prochains mois

En définitive, le GDPR – et son corollaire la protection des données – est la première priorité que se fixent les organisations pour les prochains mois et les prochaines années (priorité numéro 1 pour 73% d'entre elles).

GRAPHIQUE 3

La protection des données, priorité numéro 1 des entreprises

Priorités des entreprises



Source: IDC, 2017

Le GDPR est d'ailleurs considéré par 67% des structures interrogées comme le texte réglementaire qui impacte le plus leur politique de sécurité, loin devant le Privacy Shield (27% des structures interrogées), la directive NIS (27%) ou encore la Loi de Programmation Militaire (27%). Le Privacy Shield, entré en vigueur en septembre 2016, encadre le transfert de données vers les pays en dehors de l'Europe. La Directive NIS ("Network and Information Security"), approuvée en juillet 2016 par le parlement européen, est quant à elle destinée aux *« opérateurs de services essentiels »* et à certains fournisseurs de services numériques avec pour objectifs de renforcer les exigences de sécurité et de notification d'incidents de sécurité. La Loi de Programmation Militaire (LPM) précise quant à elle les conditions de sécurisation des systèmes d'information des OIV (Opérateur d'Importance Vitale) suivant leur secteur d'activité. Ces différents textes ne s'imposent pas à toutes les entreprises, à la différence du GDPR dont la portée est "universelle" (toutes entreprises disposant de données personnelles sur les citoyens européens).

Les résultats de l'étude menée par IDC montrent bien que, même si la priorité est à la protection des données, le chemin restant à parcourir pour être parfaitement conforme dès le 25 mai 2018 est encore sinueux. Ainsi, moins de la moitié des entreprises a formellement défini un calendrier de mise en place du GDPR tandis que 13% projettent de définir ce calendrier dans les prochains mois. Plus inquiétant : 1 interlocuteur sur 3 en charge de la sécurité informatique n'a aujourd'hui pas de visibilité sur la définition de ce calendrier, un élément qui le concerne pourtant au plus haut point. En définitive, l'enjeu pour les entreprises est de structurer une véritable gouvernance de ce projet de mise en conformité en y intégrant les différentes parties prenantes : la direction des risques et de la conformité, la direction juridique, la direction informatique et la direction de la sécurité des systèmes d'information.

VERS UNE NOUVELLE APPROCHE DE LA REMEDIATION

Répondre aux exigences du GDPR (obligation de notifier un vol de données dans un délai de 72h), et plus généralement d'ailleurs aux enjeux de sécurité, c'est surtout être capable de réagir rapidement aux menaces et aux intrusions. Bien que les entreprises soient aujourd'hui équipées d'une multitude d'outils leurs permettant de sécuriser et de surveiller leurs infrastructures, la durée moyenne entre le moment où une intrusion se produit et le moment ou l'entreprise s'en aperçoit reste relativement longue (106 jours en moyenne en Europe) alors qu'il ne faut au maximum que quelques jours aux assaillants pour réussir une intrusion lors des exercices de tests de pénétration.

La remédiation, dans le top 3 des priorités des entreprises

Dans ce contexte, **la mise en place de solutions permettant d'automatiser et d'améliorer les processus de réponses aux incidents, également appelée remédiation, remonte dans le classement des priorités de sécurité et se positionne cette année en troisième priorité de sécurité** des grands comptes interrogés (au même niveau que la sécurisation des flux applicatifs) derrière la protection des données et la protection des réseaux (voir graphique 3 ci-dessus).

Les résultats de l'enquête révèlent l'importance de renforcer la mise en place de ce type de services. Les entreprises en ont bien conscience : 76% d'entre elles ont mis en place un service de réponse aux incidents, un taux qui devrait rapidement augmenter dans les prochains mois pour atteindre 82% fin 2018 (+4% par an).

La non-identification d'une faille peut avoir des conséquences lourdes pour l'entreprise dans la mesure où elle expose les réseaux à une cyber-attaque. L'enjeu est alors de détecter – et de corriger- le plus rapidement possible les incidents qui peuvent impacter la sécurité du système d'information. Deux axes deviennent prioritaires :

- Réduire le temps moyen de détection (MTTD), qui se compte encore le plus souvent en mois pour qu'il se réduise à quelques heures ou quelques minutes.
- Réduire le temps moyen de réaction (MTTR) afin de neutraliser les cyber-attaques le plus tôt possible, et éviter ainsi qu'elles ne causent des dommages de grande envergure pour l'entreprise. Cette capacité à réduire le temps de réaction est également un levier permettant de réduire à la fois les coûts liés à l'attaque et la difficulté pour y remédier.

Expertise et automatisation, les 2 leviers d'une remédiation réussie

Dans un contexte où la principale question n'est plus de savoir si le système d'information va subir une attaque mais plutôt quand, quel sera son impact et comment y faire face, il parait essentiel pour les entreprises de se doter d'une nouvelle approche de la remédiation. Atteindre les objectifs précédemment cités (réduction du MTTD et du MTTR) nécessite de renforcer deux axes clés : le niveau d'expertise en matière de menaces et l'industrialisation de la détection et de la réaction aux menaces. Sur ces deux axes, les grandes organisations interrogées par IDC avancent à grand pas :

- Pour parfaire leur niveau d'expertise, face à la multiplication des menaces et à leur complexité croissante, les entreprises s'appuient de plus en plus sur des partenaires externes : près d'un quart des entreprises interrogées (24%) ont déjà externalisées tout ou partie de la gestion de leur service de réponse aux incidents en mettant en place des équipes mixtes (interne/ externe) ou en externalisant la totalité de ce service à un spécialiste des services de sécurité opérés.

- L'amélioration du temps de réaction suite à une tentative d'intrusion passe le plus souvent par l'automatisation. Les résultats de l'enquête montrent que les entreprises ont pris pleinement conscience qu'elles ne pourront améliorer leur capacité de remédiation qu'à travers l'utilisation d'outils adaptés. Alors que 63% des structures interrogées planifient et gèrent la réponse aux incidents de sécurité au cas par cas (de manière non automatisée), elles seront 72% à disposer de solutions automatisées dans les 2 prochaines années (voir figure 4). Une évolution justifiée par le fait que la gestion au cas par cas est particulièrement complexe, consommatrice de ressources et constitue un facteur d'allongement du temps de réaction face à une tentative d'intrusion.

Aujourd'hui, 63% des entreprises planifient et gèrent encore la réponse aux incidents de sécurité au cas par cas.

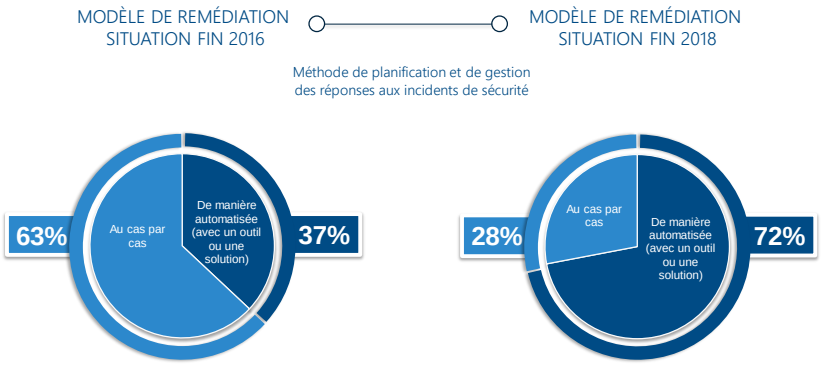
Fin 2018, 73% utiliseront des solutions automatisées

Les solutions d'orchestration et d'automatisation dédiées à la réponse aux incidents de sécurité permettent en outre de renforcer les capacités de l'entreprise à assurer la traçabilité des attaques et à contrôler l'ensemble de l'environnement de sécurité, c'est-à-dire les 40 à 50 briques technologiques qui le composent.

Une approche efficace de la remédiation implique pour les entreprises d'avoir une visibilité complète et en temps réel de leur activité réseau ainsi qu'une connaissance approfondie des événements potentiellement dangereux, dès qu'ils se produisent. L'atteinte de ces objectifs passe notamment par l'adoption de solutions globales de sécurité qui vont au-delà des outils traditionnels de prévention. Au même titre que la Business Intelligence a permis aux entreprises d'analyser l'ensemble des données et de saisir des opportunités jusque-là inconnues, les solutions modernes de "Security Intelligence" jouent le même rôle avec les informations relatives aux vulnérabilités.

GRAPHIQUE 4

Quelle approche en matière de remédiation ?



Source: IDC, 2017

Selon IDC, il est désormais essentiel de disposer d'une solution permettant la mise en place d'un ensemble de **processus pour résoudre les incidents** englobant l'ensemble du chaînage allant de **l'identification des problèmes à la mise en place de procédures de résolution et la définition de plans d'actions**.

TROUVER LE BON EQUILIBRE ENTRE LES EQUIPES, LES PROCESSUS ET LES TECHNOLOGIES

Les outils sont bien entendu une brique essentielle à la mise en œuvre d'une politique de sécurité efficace. Ils ne sont toutefois pas suffisants. La politique de sécurité doit également s'appuyer sur des processus clairement définis et sur des compétences fortes (les équipes) pour permettre à l'entreprise de renforcer sa posture de sécurité, c'est-à-dire sa capacité à résister à des attaques délibérées.

Dans ce cadre, il est nécessaire de définir une gouvernance de la sécurité des systèmes d'information qui articule le triptyque compétences / processus / technologies afin de trouver le bon équilibre entre ces 3 dimensions. Les enjeux sont nombreux :

- ***Au niveau des équipes*** : les entreprises font aujourd'hui face à une véritable pénurie de compétences et rencontrent des difficultés à retenir celles dont elles disposent actuellement. Le recours à l'externalisation auprès de fournisseurs de services spécialisés dans le domaine de la sécurité est pour nombre d'entreprises une solution qui doit permettre aux équipes internes de faire face à un nombre toujours croissant de menaces et d'alertes.

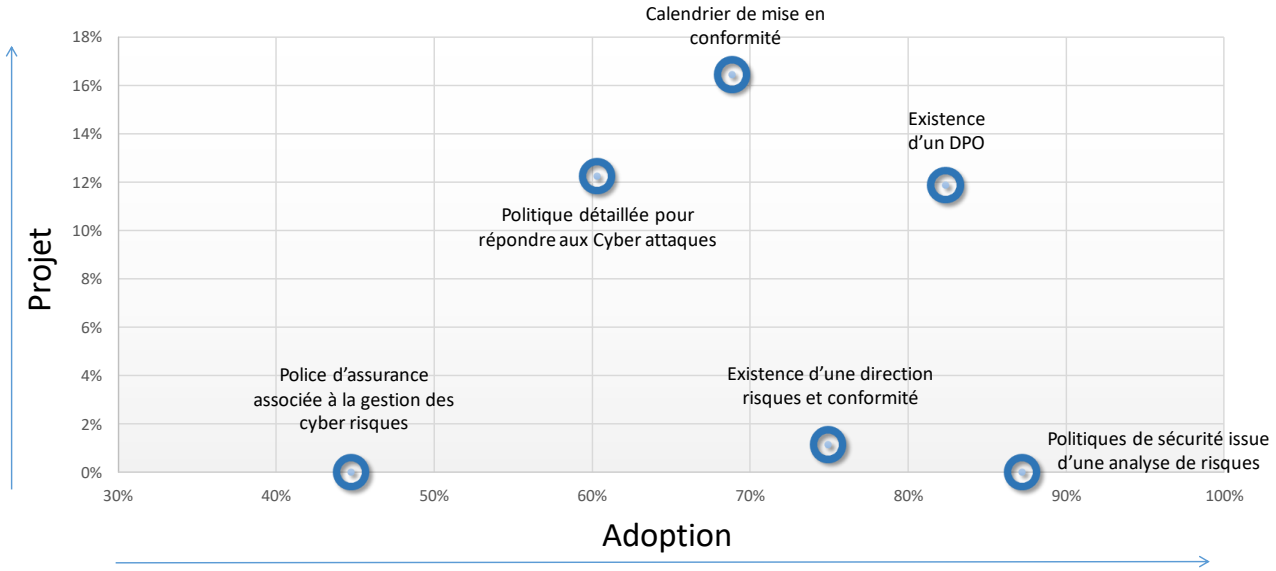
- ***Au niveau des processus*** : les entreprises doivent s'attacher à mener des audits de sécurité de manière régulière afin de mettre en place ou renforcer leur politique de réponse aux cyber-attaques. Avec la contrainte du GDPR, 2017 et 2018 seront marquées par une augmentation de ces projets : audit interne global destiné à évaluer la situation actuelle et les besoins de se mettre effectivement en conformité, cartographie pour identifier la nature des données dont elles disposent (personnelles ou pas), leurs criticités, leurs localisations, les droits utilisateurs et les usages qui leurs sont associés.

- *Du coté technologique* : les outils et solutions continuent d'évoluer en s'appuyant par exemple sur des technologies d'analyses comportementales et cognitives. L'enjeu étant de renforcer l'automatisation et de disposer d'informations très rapidement actionnables (criticité de la menace, niveau de risque, localisation, mode de propagation) pour lutter contre les menaces qui continuent de croitre.

Cette gouvernance passe notamment par un modèle organisationnel adapté : mise en place d'une direction des risques et de la conformité par exemple, ou encore mise en place d'un DPO (Data Protection Officer) en charge de la protection des données. Elle s'appuie également sur le déploiement de politiques de sécurité structurées qui donnent un cadre formel et une cohérence d'ensemble aux initiatives de sécurité : analyse des risques, audit et calendrier de mise en conformité, politique détaillée de réponse aux cyber-attaques (processus à mettre en œuvre, modèle d'alerte et d'escalade, procédures immédiates). Les grandes entreprises s'inscrivent progressivement dans cette démarche. Le graphique 5 ci-dessous montre ainsi qu'elles se focalisent désormais sur 3 axes prioritaires : la protection des données (nomination d'un DPO), la gestion de la conformité et l'organisation de la réponse aux cyber-attaques.

GRAPHIQUE 5

Critères de gouvernance de la sécurité des systèmes d'information : niveau d'adoption et projets



Source: IDC, 2017

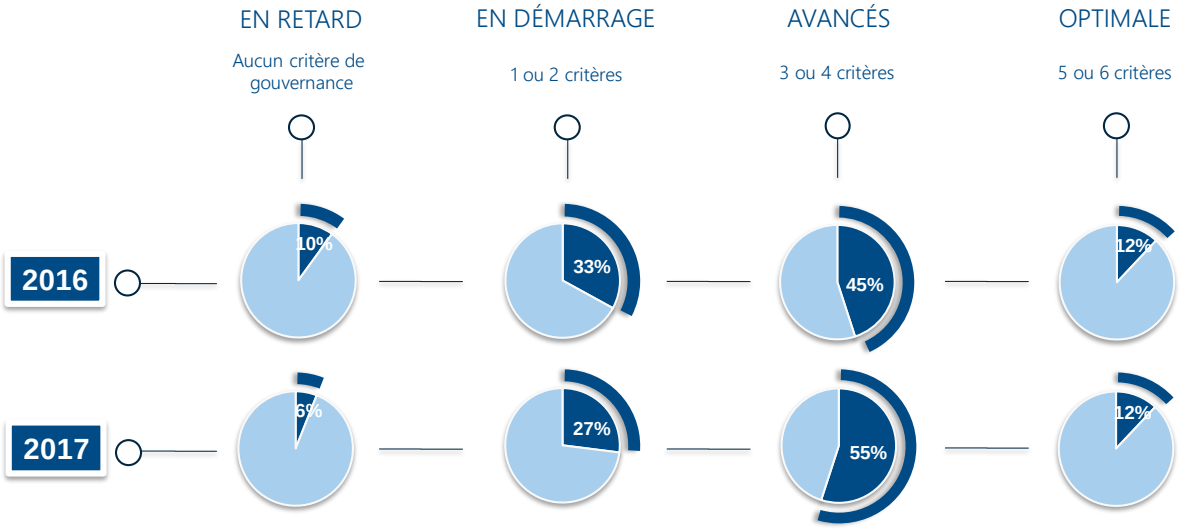
A partir des critères exposés dans le graphique 5, IDC a développé un index de la gouvernance de la sécurité afin d'évaluer le niveau de maturité des grandes organisations en France. Cet index permet de constater que la gouvernance de la sécurité est un sujet qui prend de l'envergure au sein de ces grands comptes. En effet, de nombreuses entreprises, qualifiées jusqu'alors de retardataires ou "en démarrage" (face aux peu d'initiatives qu'elles avaient menées) vont progressivement basculer vers le niveau "avancés" d'ici fin 2017 (graphique 6). Selon IDC, plus des deux tiers des organisations interrogées (67%) auront mis en place au moins 3 critères de gouvernance parmi les 6 proposés avant fin 2017.

Cette gouvernance de la sécurité des systèmes d'information se structure et implique de plus en plus d'interlocuteurs en dehors de la DSI : les Directions générales sont directement impliquées au

sein d'1 grand compte sur 3, tandis que les Directions métiers ou fonctionnelles participent dans 1 organisation sur 2. En définitive, le Comité Exécutif et les Directions métiers ne peuvent plus ignorer les risques liés aux cyber-menaces : risques économiques (perte d'exploitation liée à l'indisponibilité d'un site marchand, perte de nouveaux contrats suite au vol de données commerciales ou de données clients…), impact négatif sur la réputation et risques juridiques (la responsabilité civile et pénale du dirigeant étant engagée en cas de défaut de protection de son système d'information notamment si celui-ci entraine la divulgation de données personnelles, pénalités financières associées au GDPR).

GRAPHIQUE 6

Index de la gouvernance de la sécurité des grands comptes en France (2016-2017)



Source: IDC, 2017

EN CONCLUSION

L'une des problématiques les plus importantes dans la mise en œuvre des solutions de sécurité informatique au sein d'une organisation est la complexité même des menaces de sécurité et son corollaire, le manque de compétences en interne. Les nombreux projets de transformation numérique et les enjeux qui lui sont directement associés – sécurité des accès, des terminaux et des applications mobiles, protection des données dans un environnement Cloud – rendent la gestion de la sécurité particulièrement complexe. Les couches de sécurité s'additionnent et favorisent le développement d'un environnement souvent très hétérogène. De ce fait, l'expertise qu'il est nécessaire de maîtriser pour identifier et contrecarrer ces menaces est souvent difficile à acquérir en interne et surtout difficile à maintenir à un niveau élevé.

Ce constat pousse les entreprises à professionnaliser leurs activités de sécurité à travers 3 axes : le recours à des partenaires externes pour disposer des bonnes compétences, l'orchestration et l'automatisation croissante des réponses aux incidents de sécurité, et la mise en place d'une gouvernance en matière de sécurité. Cette évolution est accélérée par la nécessité de répondre aux exigences du GDPR dans des délais relativement courts. Les RSSI ont désormais une écoute plus importante de la Direction Générale et des Directions métiers face à ces enjeux réglementaires. Cette sensibilité nouvelle doit permettre à l'entreprise d'accélérer ses prises de décision en matière de sécurité et de protection. Conséquence directe : alors que les organisations ont dépensé en moyenne au cours des 3 dernières années 4,5% de leurs budgets informatiques en sécurité**,** cette dépense augmente désormais plus rapidement que l'enveloppe informatique globale.

A propos d'IDC

IDC est un acteur majeur de la Recherche, du Conseil et de l'Évènementiel sur les marchés des Technologies de l'Information, des Télécommunications et des Technologies Grand Public. IDC aide les professionnels évoluant sur les marchés IT et les investisseurs à prendre des décisions stratégiques basées sur des données factuelles. Plus de 1100 analystes proposent leur expertise globale, régionale et locale sur les opportunités et les tendances technologies dans plus de 110 pays à travers le monde. Depuis plus de 50 ans, IDC propose des analyses stratégiques pour aider ses clients à atteindre leurs objectifs clés. IDC est une filiale de la société IDG, leader mondial du marché de l'information dédiée aux technologies de l'information.

IDC France

13 Rue Paul Valéry
75116 Paris, France
+33.1 56.26.26.66
Twitter: @IDCfrance
idc-community.com
www.idc.com / www.idc.fr
