



Évaluer les meilleures pratiques et votre niveau de maturité SSI par rapport à vos pairs

INTRODUCTION

Gérer une entreprise au 21e siècle, équivaut à nager au milieu des requins. Le danger est omniprésent : chaque jour les hackers se développent, s'organisent et collaborent toujours plus. Pourtant, vous n'avez pas le choix : la traversée de l'océan de la transformation numérique est inévitable. Pour de nombreux dirigeants d'entreprise actuels, l'avenir de leur activité en dépend. Cela implique donc d'aller au plus profond de ces eaux infestées de requins...

Les technologies de transformation numérique – Big Data/analytique, cloud computing, mobilité et réseaux sociaux – exposent les données et les applications de l'entreprise hors du périmètre de sécurité, assuré par les contrôles au niveau du réseau et des points d'accès. Les experts en sécurité sont ainsi confrontés à une perte de contrôle et de visibilité des données. Vous nagez déjà en eaux troubles, mais voilà que la porte de la cage qui vous protégeait des requins vient de s'ouvrir.

Éviter la transformation numérique n'est pas une option. Pensez au destin d'entreprises telles que Blockbuster ou Borders, qui n'ont pas su s'adapter à la nouvelle réalité, ni comprendre ses implications. Voilà pourquoi un changement radical d'approche stratégique et technologique s'impose. Ce document vise à décrire les meilleures pratiques adoptées par vos pairs avec l'approche la plus mature en termes de sécurité. Pour pouvoir survivre au milieu des requins, voire défendre votre territoire, vous avez besoin d'une nouvelle perspective.

OBJECTIF DE CE DOCUMENT

Ce document a pour objectif de mieux comprendre les caractéristiques et l'évolution de la maturité SSI. Il identifie certains exemples de meilleures pratiques pouvant être adoptées afin d'améliorer votre propre maturité SSI. Il met également en évidence certains accélérateurs en termes d'innovation qui ont un impact particulièrement fort sur la croissance des niveaux de maturité. Enfin, il expose des recommandations sur les démarches à suivre dans le but d'améliorer votre compétitivité par rapport à vos pairs. Les informations de ce document proviennent d'une étude menée au cours de l'été 2016 auprès de 500 décideurs seniors spécialisés dans la sécurité et basés en France, en Allemagne, en Italie, en Espagne et au Royaume-Uni.

LE PROFIL DE MATURITÉ DE VOS PAIRS

Selon notre étude auprès de 500 décideurs seniors spécialisés dans la sécurité, IDC a divisé le marché en cinq catégories de maturité par ordre croissant :

- ad hoc**
- opportuniste**
- répétable**
- géré**
- optimisé**

La représentation graphique de la maturité des entreprises prend habituellement la forme d'une « courbe en cloche » classique, telle qu'illustrée ci-dessous (graphique 1).

Peu de vos pairs se situent aux extrémités dans leur approche sécurité ; au contraire la plupart se trouvent plutôt dans la moyenne. Si vous souhaitez nager au milieu des requins sans subir d'attaque, vous devriez viser un niveau supérieur et adopter les meilleures pratiques. La section suivante de ce document met en avant un aperçu des meilleures pratiques en termes de sécurité.

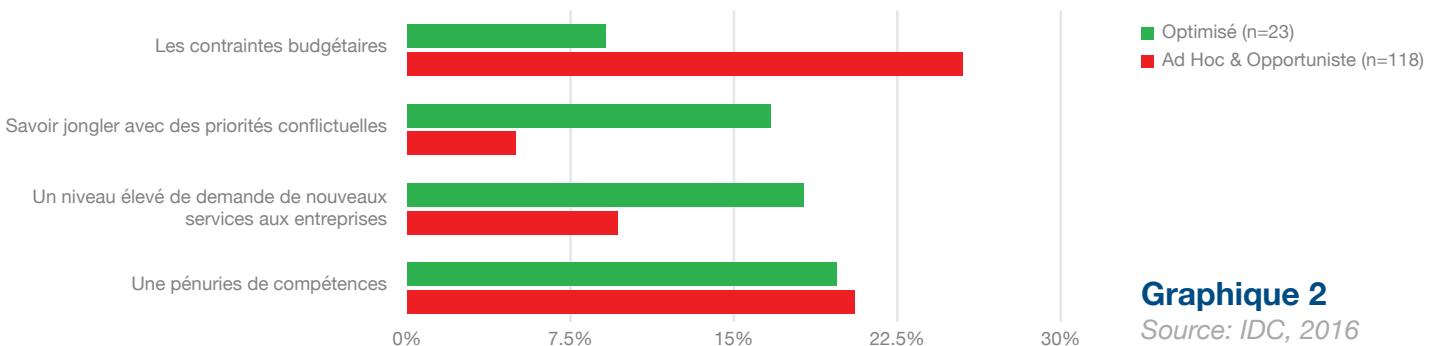
MEILLEURES PRATIQUES DE SÉCURITÉ

Traditionnellement, les technologies de sécurité étaient destinées à protéger les entreprises contre les menaces connues. En rassemblant les appareils, les applications et les données à l'intérieur du filet de sécurité du pare-feu, le contrôle du périmètre au niveau des appareils et du réseau permettait de contrer ce type de menaces. Toutefois, deux tendances rendent ces modèles de sécurité préventifs insuffisants en tant qu'approche autonome :

- La transformation numérique expose les applications et les données de l'entreprise hors du périmètre, et hors de la visibilité et du contrôle des équipes de sécurité en interne.
- L'étendue de la menace est sans précédent. Plus d'un million de nouvelles variantes de virus apparaissent chaque jour. Il est tout à fait impossible de générer des signatures à un rythme suffisant pour maintenir à jour les défenses traditionnelles destinées à bloquer les nouvelles attaques.

À l'évidence les entreprises doivent adopter de nouvelles approches pour identifier et contrer les nouvelles menaces tout en bloquant celles qui sont connues. La sécurité doit devenir proactive. Elle doit rechercher les indicateurs potentiels de risque de sécurité pour y remédier plutôt que d'attendre une nouvelle attaque. Cette démarche requiert cependant de conceptualiser la stratégie de sécurité. L'analyse des éléments qui peuvent potentiellement limiter l'efficacité de la sécurité par niveau de maturité est révélatrice, comme l'illustre le graphique 2.

Limites à l'amélioration de la sécurité des systèmes d'information par niveau de maturité



Graphique 2

Source: IDC, 2016

Certains éléments sont communs à tous les niveaux de maturité. Les coûts et la disponibilité des compétences apparaissent notamment comme les principales contraintes. Ce constat n'a rien de surprenant vu la pénurie mondiale en termes de compétences qui reste constante sur le marché de la sécurité. Toutefois, l'importance de certaines autres problématiques permet de mieux cerner les meilleures pratiques.

Pour les faibles niveaux de maturité, les contraintes de coût et la pénurie de compétences constituent les premières préoccupations. Les niveaux de maturité plus élevés recouvrent les mêmes besoins, à savoir la gestion des priorités divergentes et la prise en charge de la demande de nouveaux services d'entreprise. Ceci illustre une étape essentielle au changement de mentalité : la meilleure pratique de sécurité étant de prendre en compte les besoins de l'entreprise.

Une fois cette exigence conceptualisée, les entreprises doivent comprendre ce qu'elle implique en termes d'approche de sécurité. Le passage de modèles de sécurité réactive à une sécurité proactive est alors impératif. De fait, comme l'illustre le graphique 3, deux tendances nettes se dégagent au niveau des techniques de maturité. Plus une entreprise est mature, plus elle est susceptible d'utiliser des techniques de sécurité proactive, et plus elle aura tendance à les planifier, voire à déjà les appliquer.

Adoption d'une sécurité proactive par niveau de maturité



Graphique 3

Source: IDC, 2016

Selon notre étude, les technologies clés de sécurité que les entreprises peuvent adopter afin de faciliter ces approches plus proactives incluent la capacité d'identification des menaces, l'intelligence artificielle et l'analyse heuristique du comportement des utilisateurs. Comme avec les technologies proactives, plus l'approche d'une entreprise en matière de sécurité est mature, plus elle est susceptible d'utiliser des solutions telles que l'IA et l'heuristique.

Bien que les approches proactives de la sécurité offrent la possibilité d'élever le niveau de maturité SSI, elles présentent également un certain nombre de défis. Par exemple, les techniques proactives nécessitent de collecter et de superviser des tableaux de bord sur une plus grande échelle. Au vu des restrictions budgétaires auxquelles sont soumises les équipes de sécurité, il est nécessaire d'engager des débats constructifs sur les techniques permettant d'alléger la charge de travail des ressources internes. Les meilleures pratiques s'orientent essentiellement vers ces deux solutions potentielles.

L'EXTERNALISATION

Même si la sécurité de l'entreprise est lourde et complexe, la tendance générale est de la contrôler en interne. Plusieurs facteurs de motivation entrent en jeu. Pour commencer, la sécurité est perçue comme une activité critique. Toute externalisation est perçue comme une menace puisque cela réduira la visibilité et le contrôle des équipes internes sur leur stratégie de sécurité. Par le passé, les fournisseurs de services de sécurité gérés (MSSP) ont fait de grandes promesses, mais la réalité ne s'est pas toujours montrée à la hauteur de ces engagements. Finalement, le recours à une aide extérieure peut également être assimilé à un aveu d'échec des équipes internes, pouvant être vu comme étant incapables d'assumer seules ce type d'opération.

Pourtant, dans un monde connecté, aucune entreprise n'est totalement à l'abri, ni immunisée contre la menace. C'est notamment le cas des entreprises européennes qui possèdent des ressources en sécurité limitées, avec des prestataires externes qui bénéficient d'un positionnement accru en termes d'offre de services grâce, entre autres, à une envergure internationale, des modèles de prestations industrialisés et un meilleur accès aux compétences. Pour les entreprises qui souhaitent adopter de meilleures pratiques de sécurité, les services de sécurité gérés constituent donc une option de choix.

L'utilisation des services de sécurité gérés permet d'alléger temporairement la charge de travail des ressources internes, toutefois, l'entreprise doit également envisager d'autres solutions. L'étude d'IDC indique que, plutôt que de recourir à l'externalisation totale, la meilleure pratique consiste à trouver le juste équilibre entre services internes et services de sécurité gérés afin de répondre exactement aux objectifs commerciaux et éviter tout risques à l'entreprise. Il est important de conserver une équipe interne au sein des opérations de sécurité pour comprendre l'impact stratégique que peuvent avoir les décisions commerciales sur la sécurité, et vice-versa. Alors que la sécurité devient de plus en plus une question de gestion des risques à l'échelle de l'entreprise, elle constitue une caractéristique essentielle des meilleures pratiques pour la gestion de l'activité, pratiques de sécurité comprises.

AUTOMATISATION

Parallèlement aux services de sécurité gérés, l'automatisation est un autre levier clé que les entreprises peuvent actionner pour alléger la charge de travail des équipes et compenser le déséquilibre entre l'exigence de transformation numérique et l'évolution de la menace. L'automatisation permet de gérer et de mettre en œuvre les opérations de sécurité par le biais de produits technologiques. L'implication du personnel interne permet de garder la visibilité et le contrôle sur la sécurité.

Cette démarche aura des conséquences sur l'émergence de l'IA et de l'informatique cognitive au sein de la sécurité. L'objectif est d'alléger davantage la pression pesant sur les ressources internes en confiant la prise de décision aux machines. Toutefois, il est clair que la meilleure pratique (du moins pour l'instant) consiste à conserver un degré de supervision humaine pour garantir un bon fonctionnement des machines, ou pour avoir une maîtrise des décisions les plus critiques.