IDC Executive Brief

Sponsorisé par:
Malwarebytes

Sandrine Peyronnet
Stéphane Krawczyk

Observatoire Cybersécurité 2017:Quelles initiatives des entreprises face à la prolifération et à la complexité des menaces ?

Malwarebytes

OPINION IDC

Les résultats de l'observatoire Cybersécurité 2017 montrent que la protection des données sensibles reste la principale priorité pour 76% des entreprises en matière de sécurité IT. Elle est directement suivie par le besoin qu'ont les entreprises, à faire face à la recrudescence des attaques ciblées et la sécurisation des terminaux mobiles.

Au-delà de ce constat, IDC identifie trois principaux facteurs qui bouleversent aujourd'hui le marché de la sécurité et créent à la fois de nouvelles problématiques mais également de nouvelles opportunités pour les acteurs du marché.

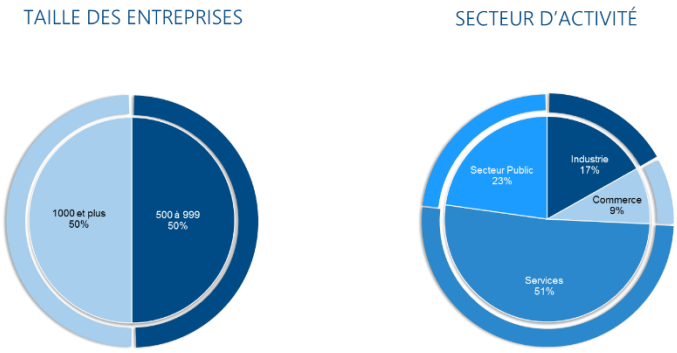
- Le premier facteur est sans aucun doute la prolifération continue des menaces qui se caractérise notamment par les centaines de milliers de nouveaux malwares découverts chaque année, la multiplication des attaques en DDOS associée à de nouvelles méthodes d'amplification, la prolifération des "rançongiciels" ou encore la professionnalisation des attaques comme dans le cas des "APT" (Advanced Persistent Threats). Face à cette évolution, les approches traditionnelles reposant sur la mise en place d'un périmètre de protection ne permettent plus à elles seules d'y faire face.
- Un second facteur concerne l'évolution de la législation autour de la protection des données en Europe mais également en France, ainsi que les obligations règlementaires spécifiques à certains secteurs d'activités qui transforme progressivement la façon dont les entreprises gèrent et protègent leurs données contre les attaques, les actes internes malveillants, ou les négligences de certains salariés ou partenaires.
- Le troisième facteur est la transformation numérique des entreprises qu'IDC illustre depuis déjà plusieurs années au travers du concept de troisième plateforme. Celle-ci repose sur quatre grands piliers technologiques : la mobilité, le cloud, les technologies analytiques ainsi que les réseaux sociaux. Ces piliers, auxquels il faut bien entendu ajouter le développement de l'internet des objets, génèrent de nouvelles possibilités mais également de nombreux défis compte tenu de l'extension de la surface d'attaque qu'engendre ce phénomène.

La conjonction de ces trois principaux phénomènes bouleverse véritablement la dynamique du marché de la sécurité. Pour répondre à ces changements, les entreprises seront amenées à adopter des solutions de sécurité de nouvelle génération et gagner en maturité sur la gouvernance de la sécurité. L'objectif étant de faire évoluer leur approche d'un modèle prévention /protection vers un modèle plus axé sur la détection et la réponse lorsque qu'un incident de sécurité survient.

METHODOLOGIE

L'observatoire de la Sécurité réalisé par IDC repose sur une enquête réalisée en juillet 2017 auprès de 200 structures basées en France et regroupant chacune plus de 500 salariés. Ces organisations sont présentes dans tous les secteurs d'activité dont les services, l'industrie, le commerce et le secteur public. Les personnes interrogées exercent des responsables dans le domaine de la sécurité des systèmes d'information et sont pour certains d'entre ainsi que des responsables métiers. 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



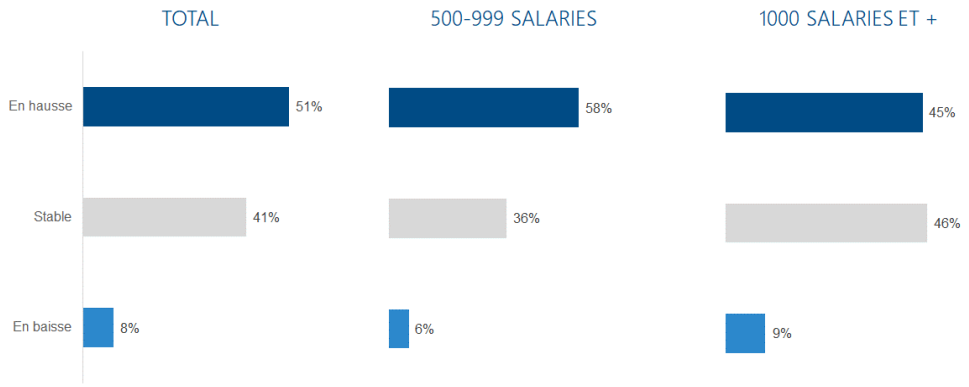
Source: IDC, 2017

UNE PROLIFERATION CONTINUE DES MENACES

Au-delà des attaques de grande envergure comme WannaCry et Peyta qui ont fait la une de l'actualité en mai et juin 2017, les cyber-attaques sont une réalité concrète dans les entreprises françaises. Elles sont d'ailleurs en hausse pour une majorité d'entreprise par rapport au nombre d'attaques qu'elles ont subies au cours de l'année 2016. Un phénomène qui ne touche pas que les très grandes entreprises mais également les PME (structures de 500 à 1000 salariés) qui constatent un regain d'activité du côté des attaques informatiques (voir graphique 2).

Graphique 2
Evolution des cyber-attaques entre 2016 et 2017

Q. Par rapport à 2016, vous diriez que les attaques subies en 2017 sont... ?



Source: IDC, 2017

Les spécialistes de la sécurité informatique au sein des entreprises ne sont plus les seuls à observer cette recrudescence des cyber-attaques. En effet, la transformation numérique croissante des différents départements de l'entreprise ouvre de nouvelles perspectives aux hackers : c'est désormais toute l'entreprise qui est impactée par ces cyber-attaques. Les directions métiers interrogées par IDC sont en effet près de la moitié à avoir constaté une hausse des cyber-attaques en 2017 alors que le chiffre issu des services informatiques est seulement de 4 points plus élevé. Ce faible écart s'explique également par le développement de la communication au sein des entreprises, et en particulier entre les directions métiers et la direction des systèmes d'information. Une cyber attaque n'est plus un sujet caché et préservé par le responsable de la sécurité des systèmes d'information.

La transformation numérique croissante des différents départements de l'entreprise ouvre de nouvelles perspectives aux hackers : c'est désormais toute l'entreprise qui est impactée par ces cyber-attaques.

Si l'on regarde plus particulièrement les attaques de ransomwares (tels que l'étaient WannaCry et Peyta), on se rend compte que cette fois-ci, ce type d'attaque touche davantage les grandes entreprises de plus de 1000 salariés (25%) que les entreprises plus petites (12%). Cet élément s'explique par la puissance financière plus importante qui motive les hackers à attaquer davantage ce type d'entreprise. Mais les grandes entreprises étant souvent hostiles à payer ces rançons, il est fort probable que les entreprises de taille intermédiaire seront à leur tour touchées dans les années suivantes par les attaques de ransomwares.

Ce qui est fondamental pour les entreprises, ce n'est pas spécialement de réduire le nombre d'attaques subies, même si c'est sous-jacent dans les actions réalisées. L'important, c'est de rester protéger contre ces attaques et de subir le moins d'impacts négatifs, que ce soit en terme financier, en terme d'image ou en matière de protection des données.

EVALUER LES IMPACTS FINANCIERS DES CYBER-ATTAQUES : UNE VRAIE DIFFICULTE POUR LES ENTREPRISES

Les résultats de l'étude montrent que les entreprises sont très nombreuses à avoir subi les conséquences négatives de ces attaques sur leur activité au cours des 12

derniers mois. Elles sont près de 70% à mettre en avant les conséquences directes de ces cyber-attaques sur leur activité : indisponibilité du site Internet de l'entreprise pendant plusieurs heures (39%), retard de livraison auprès des clients (27%) ou encore arrêt de la production pendant quelques heures.

La difficulté pour les entreprises réside dans l'identification et la mesure des conséquences financières de ces différents impacts pour l'entreprise : elles ne sont que 20% à risquer une telle analyse et à considérer que leur bas de bilan est directement touché par les cyber-attaques qu'elles subissent.

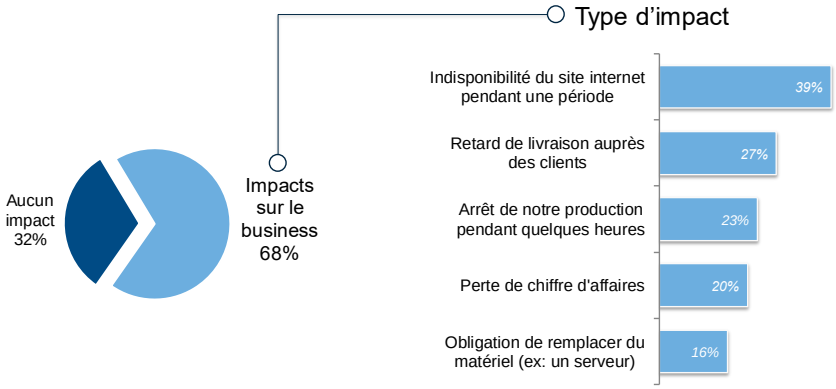
- Selon IDC, la réalité est beaucoup plus complexe. Plusieurs raisons expliquent que les impacts financiers des cyber-attaques soient aujourd'hui un sujet difficile à aborder pour les entreprises : Il est tout d'abord difficile de mesurer les conséquences financières d'une attaque sur le chiffre d'affaires ou sur le résultat d'exploitation de l'entreprise. Au-delà de l'impact direct lié par exemple à l'indisponibilité du site e-commerce de l'entreprise – relativement facile à évaluer – d'autres éléments moins tangibles peuvent également jouer de manière importante sans pour autant être facile à évaluer pour l'entreprise : la perte de confiance des clients, l'impact sur l'image de marque et sur la réputation, la perte de propriété intellectuelle ;
- Il peut être difficile pour les entreprises d'identifier la cause réelle d'un dysfonctionnement et de rapprocher par conséquent les conséquences de ce dysfonctionnement à la perte de chiffre d'affaires ;
- Par ailleurs, identifier clairement le lien entre les cyber-attaques et la baisse du chiffre d'affaires ou du résultat d'exploitation est considéré par nombre d'entreprise comme un risque. Ce lien met en avant, auprès des investisseurs et des clients, son exposition au risque et les difficultés de l'entreprise à trouver les bonnes parades au risque de cyber-attaque.

Saint Gobain a estimé, lors de la présentation de ses résultats financiers mi-2017, l'impact du ransomware NotPetya sur son chiffre d'affaires (1,1% de son chiffre d'affaires trimestrielle) et sur son résultat d'exploitation du 1er semestre (4,4% du résultats d'exploitation).

Cependant, les cultures d'entreprise évoluent : preuve en est, certaines entreprises communiquent désormais officiellement sur les impacts financiers des cyber-attaques. C'est le cas par exemple de Saint Gobain qui a estimé, lors de la présentation de ses résultats financiers mi-2017, l'impact du ransomware NotPetya sur son chiffre d'affaires (1,1% de son chiffre d'affaires trimestrielle) et sur son résultat d'exploitation du 1er semestre (4,4% du résultats d'exploitation).

GRAPHIQUE 3
Les conséquences des cyber-attaques sur l'activité de l'entreprise

Q. Quel a été l'impact des cyber attaques sur votre business ?



Source: IDC, 2017

REDUIRE LES TEMPS DE REACTION POUR LIMITER LES IMPACTS DES CYBER-ATTAQUES

Même si l'impact financier des cyber-attaques est difficile à mesurer pour les entreprises, elles mettent en place des parades leur permettant d'en limiter leurs effets. Un des principaux objectifs de ces mesures de protection est de détecter au plus tôt une faille de sécurité et de réagir au plus vite une fois une attaque identifiée. Deux axes sont alors prioritaires :

Un des principaux objectifs de ces mesures de protection est de détecter au plus tôt une faille de sécurité et de réagir au plus vite une fois une attaque identifiée.

- 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.

Même si l'idéal serait de réagir en quasi temps réel, les temps de réaction s'améliorent d'année en année. En 2017, près d'1/3 des entreprises (30%) réagissent en moins d'1 heure pour résoudre une infection générée par un malware, un laps de temps permettant le plus souvent de limiter drastiquement les impacts de ces attaques. Les PME ne sont pas en reste : elles sont 25% à réagir très rapidement à de telles attaques tandis que 71% ont besoin de 1H à 5H pour trouver une parade. Elles sont bien conscientes de ce déficit : 65% des PME ne se sentent pas du tout protégées ou de manière partielle contre les attaques de type ransomware.

A l'inverse, les grandes entreprises (plus de 1 000 salariés) ont des niveaux de maturité assez différents : alors que 37% d'entre elles, particulièrement matures, sont capables de réagir en moins d'1H, elles sont encore 16% pour lesquelles plus de 5H sont nécessaires lorsqu'il s'agit d'identifier une parade. Un laps de temps

beaucoup trop long qui permet à chaque attaque de maximiser les dommages causés dans l'entreprise. Elles sont d'ailleurs 59% des grandes entreprises à considérer qu'elles ne sont pas suffisamment protégées contre les attaques ransomware. Cette prise de conscience est le 1er facteur qui permettra aux entreprises de mener les actions correctrices nécessaires.

GRAPHIQUE 4
Perception de la protection contre les malwares

Q. Pensez-vous être protégé de façon correcte contre les attaques « Ransomwares » ?

Source: IDC, 2017

36% des entreprises interrogées par IDC indiquent qu'elles se fixent comme priorité informatique pour les 12 prochains mois de renforcer l'analyse en temps réel afin de réduire les temps de détection des attaques et les temps de réaction de l'entreprise.

Il reste donc du chemin à parcourir pour que les entreprises se sentent totalement protégées contre les cyber-attaques en général et les ransomwares, en particulier. Les entreprises, et en particulier les responsables de la sécurité informatique, doivent faire des choix parmi l'ensemble des solutions qui existent de manière à être en parfaite adéquation avec les priorités des dirigeants d'entreprises et ainsi mettre en place les actions et/ou les outils les plus pertinents possibles. D'ailleurs, 36% des entreprises interrogées par IDC indiquent qu'elles se fixent comme priorité informatique pour les 12 prochains mois de renforcer l'analyse en temps réel afin de réduire les temps de détection des attaques et les temps de réaction de l'entreprise.

RANSOMWARE, GDPR, CLOUD, TEMPS REEL : LES PRIORITIES DES ENTREPRISES EN MATIERE DE SECURITE EVOLUENT

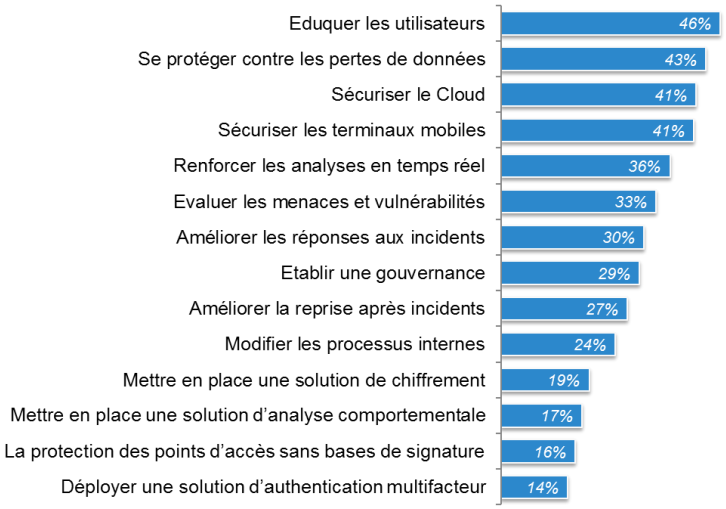
Afin de réduire les impacts négatifs des cyber-attaques, les actions à mettre en place sont très nombreuses car les attaques sont multiples et variées. Il y a énormément de possibilités d'actions et pour ne pas se perdre, les services informatiques doivent définir des priorités en termes de sécurité informatique.

La première priorité des entreprises consiste tout "simplement" à éduquer les utilisateurs pour les familiariser avec les règles et les politiques de sécurité informatique mises en place par l'entreprise. Pendant de nombreuses années, les utilisateurs se sont d'ailleurs affranchis des problématiques de sécurité informatique, celles-ci étant gérés de manière unilatérale par le département informatique et celui de la sécurité IT. Cependant, à l'aune de la transformation numérique des entreprises et de l'évolution réglementaire vers la mise en place du GDPR au niveau européen (règlement général sur la protection des données), la

problématique de sécurité devient un sujet d'importance pour les directions métiers.

GRAPHIQUE 5
Priorités en matière de sécurité IT pour les 2 ans à venir

Q. Quelles sont les priorités de votre entreprise en termes de sécurité IT pour les 2 prochaines années ?



Source: IDC, 2017

La protection des données, dans le top 3 des priorités en matière de sécurité IT

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.

Lutter contre les malwares pour renforcer la protection des données

Il s'agit désormais de changer les habitudes des utilisateurs pour que la sécurité informatique et la protection des données deviennent des réflexes pour l'ensemble des collaborateurs. C'est un projet de long terme qui est devenu encore plus sensible avec l'arrivée prochaine du GDPR en Europe en mai 2018. Les résultats de l'enquête montrent d'ailleurs que les entreprises sont largement impactées par la mise en conformité en matière de protection des données : plus de la moitié des structures interrogées (55%) identifient des impacts forts tels que la baisse des budgets consacrés aux nouveaux projets, voir dans certains cas le report des projets, afin de financer la mise en conformité GDPR. D'autres (20%) considèrent qu'elles devront changer de fournisseurs de solutions (Cloud, CRM, ERP, messagerie, collaboratifs, hébergement, infogérance ...) pour assurer leur conformité.

Les PME sont les plus en retard sur le sujet de la mise en conformité GDPR : seules 32% d'entre elles ont défini un calendrier de mise en conformité pour répondre aux évolutions réglementaires, contre 51% des grandes entreprises.

Les PME sont les plus en retard sur le sujet de la mise en conformité GDPR : seules 32% d'entre elles ont défini un calendrier de mise en conformité pour répondre aux évolutions réglementaires, contre 51% des grandes entreprises. Au-delà de ce calendrier, les entreprises investissent massivement dans de nouvelles solutions de sécurité IT pour réduire leur exposition aux risques et empêcher la fuite de données personnelles.

Renforcer et automatiser les stratégies de sécurité pour faire face aux menaces

Outre les actions prioritaires évoquées précédemment, les outils sont un autre moyen de se protéger des attaques que peuvent rencontrer les entreprises. Les logiciels de protection des points d'accès (Endpoint Security) tels que les antivirus, anti spyware, chiffrement de fichier ou de disque, font partie des équipements les

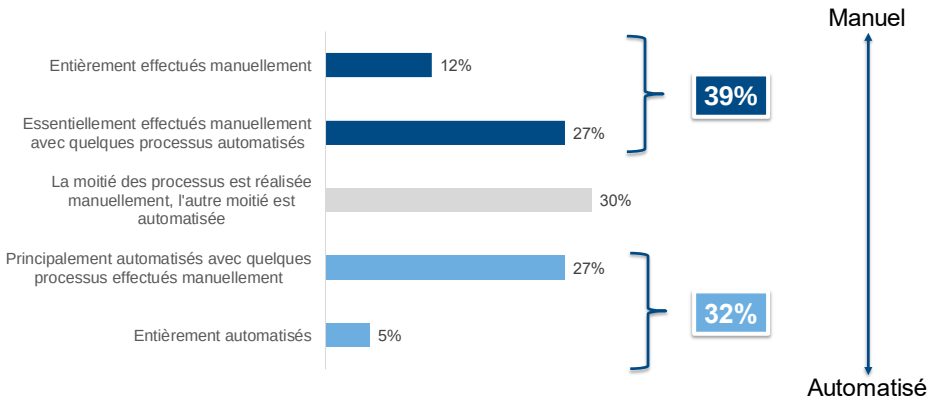
plus déployés par les entreprises : 53% des structures interrogées les ont déployés tandis que 28% sont en phase de déploiement. Elles sont par ailleurs 16% à projeter de tels déploiements dans les mois à venir.

En définitive, le taux d'utilisation des solutions de sécurité Endpoint devrait frôler les 100% d'ici 24 mois. Ces logiciels de protection sont d'autant plus stratégiques que les pirates informatiques ciblent désormais prioritairement les utilisateurs finaux à travers des stratégies évoluées : il suffit pour les pirates de compromettre la sécurité d'un seul environnement utilisateur pour pénétrer l'ensemble du système. En conséquence, les solutions déployées couvrent un nombre croissant de points d'accès : 20% des entreprises déclarent protéger désormais plus de 500 points d'accès tandis que 47% protègent entre 50 et 500 points d'accès.

Au-delà des outils, les stratégies informatiques mises en place par les entreprises font de plus en plus place à des processus automatisés. En effet, face à la recrudescence des attaques et à la pénurie de ressources pour gérer la complexité croissante des menaces, l'automatisation des processus de gestion de la sécurité permet aux entreprises de réduire leur temps de réaction face aux menaces tout en traitant un volume important de menaces. Par ailleurs, la mise en place de processus automatisés permet aux services informatiques de libérer leurs équipes pour qu'elles se consacrent davantage à la définition même de la politique de sécurité et à l'éducation des utilisateurs, priorité numéro 1 des entreprises.

GRAPHIQUE 6
Evolution de l'automatisation de la sécurité

Q. Où en est votre entreprise vis-à-vis de l'automatisation des processus de gestion de la sécurité ? Vous diriez qu'ils sont…?



Source: IDC, 2017

Même si l'automatisation complète des processus de gestion de la sécurité ne sont entièrement automatisés que pour 5% des entreprises, la situation va s'accélérer très rapidement : alors que 88% des entreprises interrogées ont commencé à automatiser leurs processus de sécurité, près des 3/4 d'entre elles (72%) prévoient de renforcer dans les mois à venir le niveau d'automatisation de leurs processus de gestion de la sécurité IT.

CONCLUSION

Comment faire face à des problématiques de sécurité de plus en plus prégnantes – la transformation numérique des entreprises prend de l'envergure – et face à des ressources souvent insuffisantes pour couvrir l'envergure des besoins et la professionnalisation des attaques. Une équation particulièrement complexe, tout aussi complexe que la gestion même de la sécurité : sécurisation des accès, des terminaux et des applications mobiles, ou encore protection des données dans un environnement Cloud. Seul point positif : les RSSI ont de plus l'attention de la Direction Générale de leur entreprise dans la mesure où les impacts financiers et légaux (GDPR) deviennent sensibles, même s'ils sont encore difficiles à évaluer précisément.

Face à cette problématique, les entreprises cherchent à professionnaliser leur approche de la sécurité à travers plusieurs axes : le premier d'entre eux est l'automatisation des processus de gestion de la sécurité. Celle-ci va progressivement s'appuyer sur l'utilisation de solutions d'intelligence artificielle et d'analyse comportementale pour limiter l'action humaine dans le processus d'identification et de traitement des menaces. Le développement de la sécurité en mode Cloud est également un levier d'action de plus en plus utilisé par les entreprises (75% d'entre elles).

En définitive, cette nouvelle complexité des menaces et des solutions permettant d'y remédier impose aux entreprises de définir une nouvelle gouvernance en matière de sécurité informatique : les deux tiers des structures interrogées font évoluer l'organisation de cette gouvernance pour y intégrer la Direction générale de l'entreprise et la Direction des risques et de la conformité. En conséquence, cette gouvernance repose de plus en plus sur une politique de sécurité issue d'une analyse des risques (63% actuellement et 26% en projet). La politique de sécurité n'est désormais plus uniquement portée par le RSSI, elle est décloisonnée pour laisser une place de choix aux directions métiers, impactées en 1er lieu par les menaces de sécurité.

A propos de Malwarebytes

Malwarebytes protège de manière proactive les particuliers et les entreprises contre les menaces telles que les malwares, les ransomwares et les exploits qui échappent ála vigilance des solutions antivirus traditionnelles. Le produit phare de l'entreprise combine des fonctionnalités avancées pour la détection, la protection et la suppression des programmes malveillants.

Plus de 10 000 entreprises à travers le monde utilisent les technologies Malwarebytes. Fondée en 2008, la société est basée en Californie, avec des bureaux en Europe et en Asie, et emploie une équipe internationale de chercheurs spécialisés dans les menaces et des experts en sécurité.

Pour plus d'informations : www.malwarebytes.com

PLUS D'INFOS

Web: www.malwarebytes.com/business

Linkedin: linkedin.com/company/malwarebytes

Twitter: twitter.com/malwarebytes

Facebook: facebook.com/Malwarebytes/

Phone: +33 (800) 909-009

E-Mail: frsales@malwarebytes.com

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

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