Bien que les dépenses en matière de sécurité se maintiennent dans l'ensemble, les investissements dans ce domaine font l'objet d'un examen minutieux. L'importance stratégique croissante de la cybersécurité suscite l'attention et requiert la participation des PDG et des cadres dirigeants.

État de la cybersécurité compte tenu des menaces et des incertitudes économiques actuelles

Octobre 2023

Questions : GoSecure

Réponses : Cathy Huang, directrice de recherche, *Security Services Worldwide* (Services Sécurité à l'international)

Q. Où en est le secteur de la cybersécurité aujourd'hui ?

R. La cybersécurité a incontestablement gagné en importance stratégique au fil des ans. Au cours des deux dernières décennies, les entreprises se sont davantage appuyées sur la technologie pour améliorer l'expérience client, leur fonctionnement opérationnel, la gestion de leur chaîne d'approvisionnement ou encore la productivité de leurs collaborateurs, en utilisant principalement la technologie pour bénéficier d'un avantage concurrentiel. Pendant la pandémie de COVID-19, par exemple, les entreprises ont su utiliser efficacement les technologies et l'infrastructure numériques pour favoriser le recours au travail à distance. Une étude d'IDC révèle que 49 % des entreprises ont observé des augmentations de productivité pouvant atteindre 24 % grâce aux investissements dans la transformation numérique. En effet, de nombreux chefs de file du secteur de la technologie ont été félicités pour leurs efforts visant à fournir la disponibilité et la résilience essentielles au maintien de la continuité des activités essentielles.

Toutefois, la transformation numérique ne s'est pas déroulée sans heurts. Entre autres, le travail à distance et l'adoption croissante des solutions infonuagiques augmentent considérablement la surface d'attaque et introduisent des vulnérabilités latentes dans les réseaux domestiques ou distants. De même, les départements informatiques manquent de visibilité sur de nombreux appareils présents sur le réseau de l'entreprise, à l'origine de nouveaux risques en matière de cybersécurité. Par conséquent, les risques de cybersécurité se multiplient rapidement, donnant lieu à des brèches de données, des perturbations et des dommages coûteux pour l'entreprise.

Les évolutions en matière de cybersécurité se sont avérées d'autant plus pertinentes que les entreprises qui se sont engagées dans un processus de transformation numérique se rendent compte que leur existence même peut dépendre de leur capacité à faire face aux cyberattaques et à rétablir un état de fonctionnement viable dans les plus brefs délais. Au cours d'une année telle que 2023, de nombreuses entreprises sont confrontées à un stress financier sans précédent en raison de l'inflation et de l'incertitude économique. Bien que les dépenses en matière de sécurité se maintiennent dans l'ensemble, les investissements dans ce domaine font l'objet d'un examen minutieux. Les PDG et les cadres dirigeants attendent désormais des indicateurs et des mesures de résultats clairs afin d'évaluer et de valider les investissements réalisés dans les programmes de sécurité de leur entreprise.

Q. Dans quelle mesure la situation en matière de sécurité diffère-t-elle des années précédentes et que nous réserve l'avenir ?

R. Le nombre de cybercriminels ne cesse d'augmenter en raison des bénéfices importants, qu'il s'agisse de gains financiers, d'espionnage d'entreprise ou d'avantages économiques accordés par des acteurs soutenus par des États. Outre les cyberattaques motivées par l'argent, les tensions géopolitiques ont entraîné une recrudescence des attaques hacktivistes de nature politique.

IDC suit les activités des rançongiciels depuis le premier semestre 2021. Depuis juillet 2021, force est de constater que le nombre d'attaques par rançongiciels à travers le monde a considérablement augmenté, tout comme les paiements qui en découlent. La progression de la numérisation a considérablement étendu les surfaces d'attaque et mis en évidence les lacunes des pratiques de sécurité traditionnelles et des stratégies de sécurité réactives. À titre d'exemple, en février 2023, la série d'attaques par rançongiciels VMware ESXi qui a affecté plus de 3 800 serveurs avait exploité une vulnérabilité vieille de deux ans. Il s'est avéré que de nombreux clients utilisaient des versions obsolètes ou non corrigées du logiciel VMware ESXi.

Les rançongiciels présentent une menace sans frontières qui ne semble pas faiblir en 2023. Le paysage des rançongiciels a gagné en complexité et en technicité, à mesure que les cybercriminels trouvaient de nouveaux modes d'action. L'un des groupes de pirates les plus connus exploitant des rançongiciels, LockBit, a fait peau neuve et a remanié son entreprise affiliée après plusieurs années de mauvaise presse. Le groupe a même lancé le premier programme de primes aux bogues, qui prévoit des récompenses allant jusqu'à 1 million de dollars pour les vulnérabilités qu'il est en mesure d'exploiter. Son dernier logiciel malveillant, LockBit 3.0, peut se propager ou se répandre dans le réseau de la victime sans aucune intervention humaine.

Les rançongiciels ne sont que la partie émergée de l'iceberg si l'on considère l'ensemble du paysage des menaces renforcées. Les menaces persistantes avancées (MPA), l'hameçonnage, les brèches de données, la compromission de courriels professionnels, le déni de service et autres cyberattaques sont devenus monnaie courante. L'une des évolutions les plus inquiétantes est l'augmentation des cyberactivités malveillantes visant les systèmes industriels (par exemple, le maliciel *Industroyer*), qui représente une menace considérable pour les services vitaux accompagnant notre vie quotidienne. Il existe un risque alarmant que le monde soit confronté à un cyberincident majeur comparable à la « COVID-19 », causé par un adversaire qui exploiterait l'intelligence artificielle (IA) et les outils d'IA générative pour concevoir des cyberattaques beaucoup plus dangereuses, susceptibles de causer des dommages sans précédent.

Q. Comment se présentera le domaine de la cybersécurité compte tenu du contexte économique actuel et des obstacles auxquels les entreprises sont confrontées en raison de la dégradation de l'économie ?

R. Bien que l'économie soit un domaine imprévisible, de nombreux PDG se préparent à poursuivre leurs investissements dans la stratégie numérique de leur entreprise. Au cours de l'enquête annuelle *CEO Sentiment Survey* réalisée par IDC au début de l'année 2023, 87 % des PDG interrogés à travers le monde ont déclaré vouloir maintenir ou augmenter leurs

dépenses en matière de technologie en 2023. En outre, les technologies utilisées pour « la sécurité, le risque et la conformité » sont considérées comme les composantes les plus à l'abri des coupes budgétaires en 2023. Ces chiffres montrent que les menaces de cybersécurité et les questions de conformité, au cœur des préoccupations, sont considérées comme représentant le risque le plus important pour les PDG.

Toutefois, compte tenu des difficultés macroéconomiques actuelles qui laissent entrevoir un ralentissement de l'économie, les entreprises ne peuvent pas se permettre d'augmenter les dépenses de sécurité au rythme de leurs progrès dans leur processus de transformation numérique. Qui plus est, l'exposition au risque augmente à mesure que les entreprises tardent à décider des dépenses à engager, et que le budget consacré à la sécurité diminue. Les entreprises pâtissent du manque de talents disponibles dans le domaine de la cybersécurité. Cette pénurie reste un enjeu majeur qui ne devrait pas se résoudre de sitôt.

Chaque entreprise présente un profil de risque et une appétence pour le risque différents. Cette position fluctuante à l'égard du risque est due au secteur d'activité de l'entreprise et à sa présence géographique. De plus, l'approche d'une entreprise à l'égard du risque détermine bien souvent ses priorités en matière d'investissement. Prenons l'exemple des licenciements et des restructurations qui ont eu lieu ces derniers mois dans le secteur de la technologie. Certains PDG pourraient hésiter à investir dans de nouveaux projets, compte tenu des perspectives économiques incertaines. Cependant, d'autres PDG peuvent percevoir la situation actuelle comme une occasion d'investir dans des domaines clés et de nouvelles technologies telles que l'intelligence artificielle et l'apprentissage machine (AM) afin de conférer à leur entreprise un avantage concurrentiel.

Q. Compte tenu du caractère dynamique de la cybersécurité, comment les entreprises peuvent-elles préparer l'avenir ?

R. Les entreprises de toutes tailles, et en particulier les petites et moyennes entreprises, peinent à mettre en place des programmes de cybersécurité rentables et à l'épreuve du temps. Pour répondre aux difficultés et aux multiples problématiques de l'entreprise numérique moderne, les entreprises ont besoin d'un programme de cybersécurité personnalisable, intégré et pérenne. Ce programme doit permettre d'adopter une posture solide en matière de cybersécurité, de soutenir la cyberrésilience et de favoriser l'atteinte des objectifs de cybersécurité et de conformité, et ce, de manière rentable. Pour ce faire, il convient de mettre en place un programme global comprenant de nombreuses solutions de sécurité capables de s'intégrer à l'infrastructure informatique existante, ainsi que le personnel adéquat pour configurer, entretenir et gérer les solutions.

Un programme intégré de cybersécurité nécessite une approche exhaustive qui couvre de multiples aspects de la sécurité et des technologies associées. Par exemple, les systèmes de surveillance de sécurité performants offrent une large visibilité sur les terminaux et les réseaux, ce qui permet de collecter des signaux de sécurité et des données télémétriques afin d'améliorer l'efficacité des outils de détection des incidents. En parallèle, l'élimination des outils de sécurité cloisonnés réduit le délai de détection des menaces destructrices telles que les rançongiciels, ainsi que des menaces internes insidieuses, de reconnaissance et des vols de données.

Dans le cadre de la dernière enquête mondiale réalisée en février 2023 par IDC à partir d'une source primaire sur les services de sécurité (sur un échantillon total de 1 214 entreprises à travers le monde), 61 % des personnes interrogées ont indiqué avoir mis en place une stratégie de cyberrésilience et avoir déployé des technologies connexes dans

l'ensemble des fonctions. Toutefois, seulement 20 % d'entre elles soumettraient leur plan de cyberrésilience à des tests réguliers. Si le plan est rarement vérifié ou se limite à un document statique sans possibilité d'intégration des enseignements tirés, l'efficacité du plan de cyberrésilience peut être remise en question.

Q. Comment les futures tendances en matière de cybersécurité sont-elles prises en compte dans les prévisions de planification stratégique ?

R. Avant de connaître l'enthousiasme suscité par l'IA générative, le secteur de la cybersécurité utilisait déjà depuis un certain temps différents types de techniques d'intelligence artificielle, d'apprentissage automatique et d'analyse prédictive. La première prédiction de l'*IDC FutureScape : Worldwide Future of Trust 2023 Predictions* (IDC n° US49755022, octobre 2022), concerne les centres d'opérations de sécurité (COS) autonomes : **« D'ici 2026, 30 % des grandes entreprises migreront vers des centres d'opérations de sécurité autonomes. »**

La mobilisation de plusieurs plateformes intégrées et coordonnées permettant aux entreprises de bénéficier d'informations automatisées sur l'architecture, les menaces/vulnérabilités, les risques, les politiques et les normes aura des répercussions considérables. Les COS autonomes peuvent fournir des informations sur les menaces qui pourraient échapper à la vigilance d'une équipe de cybersécurité surchargée et harassée, ou qui dépasseraient les lignes de défense traditionnelles. IDC croit fermement que les grandes entreprises, notamment celles qui disposent de systèmes conséquents basés sur le nuage, envisageront d'investir dans des COS autonomes pour épauler leur équipe de cybersécurité.

À court terme, il faut s'attendre à ce que l'utilisation de l'IA générative accélère la tendance du COS autonome, dans la mesure où ce dernier repose sur l'utilisation de l'IA/ AM dans la détection, l'orchestration, l'automatisation et la réponse en matière de sécurité. À titre d'exemple, les entreprises peuvent utiliser l'IA/ AM pour procéder à une analyse continue du paysage des menaces en vue de détecter les nouvelles menaces et les menaces émergentes, ce qui garantirait l'identification, le triage et la remédiation des menaces à grande l'échelle.

De plus, l'utilisation de l'IA générative apportera des changements importants à l'interface utilisateur des plateformes COS autonomes. L'IA générative se fonde sur un ensemble de modèles fondamentaux non supervisés et semi-supervisés capables de créer un nouveau contenu à partir de données générées antérieurement, telles que du texte, de l'audio, des images et du code. L'adoption accélérée de l'IA générative propulsera l'IA du rang d'élément logiciel récent de la pile technologique à celui de technologie de base au cœur d'une plateforme de transition vers l'IA généralisée.

Présentation de l'analyste

Cathy Huang, *Directrice de recherche, Security Services Worldwide (Services de Sécurité à l'international)*

Cathy Huang est directrice de recherche au sein du pôle *Security and Trust research* d'IDC, axé sur les services de sécurité gérés, le conseil en sécurité et les services d'intégration dans le cadre du programme de services de sécurité. De plus, elle collabore avec d'autres membres de l'équipe en vue d'examiner les services qui permettent aux entreprises d'adopter des technologies émergentes telles que la périphérie, la 5G et l'IdO , ainsi que des domaines d'intérêt clés tels que la sécurité du nuage, la cyberrésilience et la cybertransformation.

MESSAGE DU COMMANDITAIRE

GoSecure

Chef de file incontesté du secteur de la cybersécurité, GoSecure propose des solutions de détection et de réponse étendues gérées (MXDR) ainsi que des services professionnels. Depuis plus de 10 ans, GoSecure explique à ses clients comment mieux comprendre leurs lacunes en matière de sécurité, améliorer les risques organisationnels et renforcer leur posture de sécurité grâce à des services consultatifs fournis par l'une des équipes les plus fiables et les plus compétentes du secteur. Découvrez comment les solutions MXDR de GoSecure permettent aux entreprises d'être bien équipées pour naviguer dans un paysage de menaces en constante évolution.

IDC Custom Solutions

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, États-Unis
Tél. : +1 508 872 8200
Fax : +1 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com