Les huit éléments essentiels de la cybersécurité

Publié le 15 avril 2024

Mobeen Tahir
Director, Research

- Les risques de cybersécurité augmentent à mesure que les organisations adoptent des outils numériques.
- La cybersécurité englobe une multitude d'aspects, de la protection des données à celle des appareils, en passant par la formation des utilisateurs.
- Les entreprises qui adoptent une approche holistique couvrant plusieurs aspects de la cybersécurité ont potentiellement plus de chances de perdurer dans un secteur en constante évolution.

Le 19 février, le Financial Times a signalé1 que des cybercriminels nord-coréens se tournaient vers l'intelligence artificielle (IA) pour dérober des fonds et des technologies de pointe à plusieurs victimes à travers le monde. Ce rapport décrit la manière dont les pirates informatiques ciblent les entreprises mondiales de défense, de cybersécurité et de cryptomonnaie en piégeant les victimes sur des plateformes populaires telles que LinkedIn. Il rapporte également qu'OpenAI, développeur de ChatGPT, et son investisseur Microsoft ont confirmé que des acteurs malveillants utilisaient leurs services d'IA dans le cadre de cyberactivités malveillantes.

Les outils d'IA générative ont démocratisé l'accès à des capacités techniques avancées, permettant à des individus aux compétences relativement basiques d'accomplir des tâches sophistiquées. Par ailleurs, les grands modèles de langage offrent aux utilisateurs la possibilité de communiquer avec l'ordinateur dans une langue telle que l'anglais, et de laisser le modèle traduire leurs instructions pour écrire des programmes. Malheureusement, ces technologies facilitent aussi la perpétration d'actes illicites par des acteurs malveillants. C'est pourquoi la cybersécurité doit devenir plus intelligente et résoudre toutes les vulnérabilités avant qu'elles ne soient exploitées par de tels acteurs.

WisdomTree s'est associé au groupe de capital-risque Team8 pour identifier huit domaines distincts de la cybersécurité qui sont essentiels dans un monde présentant des risques toujours croissants.

Pour être réellement efficace, la cybersécurité doit adopter une approche holistique

Source : WisdomTree, Team8, 2024.

Sécurité des données

D'après les estimations, le monde produit quotidiennement 328 millions de téraoctets de données. Un téraoctet est égal à 1 000 gigaoctets. En d'autres termes, le monde produit une quantité massive de

données. En outre, la vitesse à laquelle ces données sont produites ne cesse d'augmenter. On estime également que 90 % des données mondiales ont été générées au cours des deux dernières années seulement2.

IBM indique que le coût moyen d'une violation de données en 2023 a atteint 4,45 millions de dollars, soit une augmentation de 15 % en trois ans3. Dans un contexte où la production d'informations connaît une croissance sans précédent, la sécurité de celles-ci devient une priorité absolue. C'est précisément l'objectif des mesures de sécurisation des données.

Sécurité du cloud

La croissance exponentielle des données entraîne une demande accrue de stockage dans le cloud. Selon un rapport4, environ 60 % de toutes les données d'entreprise sont stockées dans le cloud, contre seulement 30 % en 2015. En outre, 89 % des entreprises utilisent une approche multi-cloud, un terme qui désigne une entité utilisant au moins deux applications basées sur le cloud.

Malheureusement, les acteurs malveillants en sont pleinement conscients. En 2023, il a été enregistré une hausse de 110 % des cas où l'acteur de la menace a l'intention d'accéder à un environnement en nuage pour en tirer profit, illustrant l'essor fulgurant de cette technologie5. Cela signifie que les cyberadversaires ciblent davantage les applications basées dans le cloud pour mener leurs attaques. Par conséquent, la sécurisation du cloud figure parmi les thèmes essentiels de la cybersécurité.

L'approche « Shift-Left »

La sécurisation du cloud ou de toute autre application doit être intégrée dès la conception initiale et ne peut pas être reléguée à une phase ultérieure du processus de développement. L'approche « Shift-Left » consiste à intégrer la cybersécurité dès la phase de développement d'un logiciel. L'approche inverse consisterait à faire de la cybersécurité une préoccupation secondaire, en s'appuyant sur des solutions génériques de fournisseurs tiers.

Le fait d'intégrer la cybersécurité dès le début du cycle de développement permet aux développeurs d'évaluer de manière critique les vulnérabilités dans le logiciel pour s'assurer que toutes les barrières nécessaires sont en place lors de sa création. Cette approche permet de réduire les coûts et d'accélérer la livraison, en limitant les problèmes potentiels qui pourraient survenir une fois que le logiciel est mis entre les mains des utilisateurs.

Une sécurité plus intelligente

L'accessibilité accrue de l'IA générative a ouvert la voie à une augmentation du nombre d'acteurs malveillants. Il est désormais plus facile de créer des codes nuisibles, comme ceux utilisés dans une opération dite polymorphe, dans laquelle la cyberattaque modifie le code, le contenu et la structure pour éviter d'être détectée par les systèmes de sécurité. Si un tel code est bloqué par les systèmes de sécurité d'une entreprise, il peut évoluer et devenir plus robuste.

La lutte contre ces menaces nécessite une forme d'automatisation. Une sécurité plus intelligente comprend des outils d'automatisation capables de surveiller les réseaux pour détecter les menaces potentielles. Dans ce contexte, les outils d'IA qui apprennent, s'adaptent et évoluent jouent un rôle crucial pour assurer la sécurité.

Sécurité des objets

L'Internet des objets (IdO) fait référence à l'ensemble des appareils connectés à Internet. Alors que les ordinateurs et les téléphones portables en sont des exemples évidents, l'IdO élargit considérablement la gamme des appareils concernés, englobant désormais des objets tels que les voitures, les montres, les assistants numériques, les téléviseurs ou les lave-vaisselles. D'après les estimations, il existe actuellement 17 milliards d'appareils IdO dans le monde, et ce nombre pourrait doubler d'ici 20306.

De toute évidence, nos appareils doivent être protégés dans la mesure où ils fournissent tous aux attaquants des points d'entrée pour accéder à nos réseaux et données. La sécurité des objets consiste donc à protéger ce nombre croissant de dispositifs connectés contre les menaces potentielles.

Un monde sans périmètre

Depuis la pandémie de COVID-19, la surface d'attaque s'est étendue en raison de l'augmentation du nombre d'employés travaillant à distance. La notion de surface d'attaque fait référence à la somme des vulnérabilités que les pirates informatiques sont susceptibles d'exploiter pour accéder au réseau ou aux données sensibles d'une organisation. Alors qu'auparavant, les travailleurs étaient généralement confinés à un périmètre, les attaquants bénéficient désormais d'une multitude de points d'entrée potentiels.

Dans un monde sans périmètre, les organisations ont besoin d'outils plus sophistiqués pour se protéger. Cela inclut l'authentification à deux facteurs et la biométrie qui permettent aux utilisateurs de se connecter au réseau et aux applications de leur entreprise.

Résilience et récupération

En mai 2017, l'attaque du rançongiciel WannaCry a coûté 92 millions de livres sterling au National Health Service du Royaume-Uni en raison des services indisponibles et des coûts informatiques. Plus important encore, 19 000 rendez-vous ont été annulés, car plus de 80 fiducies hospitalières et 8 % des cabinets de généralistes ont subi des perturbations7.

Selon Team8, la cybersécurité doit évoluer au-delà des approches traditionnelles consistant à « identifier, protéger, détecter et répondre », pour inclure des mécanismes de récupération rapide en cas de dégradation, de perturbation ou de refus d'accès au réseau ou aux données d'une organisation. Ne pas être capable de le faire peut avoir des conséquences catastrophiques.

Une organisation peut disposer des outils de cybersécurité les plus puissants pour se protéger, mais si les humains ne sont pas formés et équipés pour gérer les risques, les barrières de protection peuvent s'effondrer comme un château de cartes. Ainsi, la couche 8 fait référence au facteur humain.

Selon CrowdStrike, 75 % des attaques en 2023 étaient exemptes de logiciels malveillants, contre 40 % en 2019. Les attaquants délaissent de plus en plus les attaques de logiciels malveillants via des e-mails d'hameçonnage au profit de méthodes plus élaborées comme l'ingénierie sociale, qui ciblent les vulnérabilités humaines. Ainsi, le fait de permettre aux individus de mieux gérer les risques de cybersécurité pourrait constituer la pierre angulaire de toutes les autres mesures de sécurité.

Conclusion

La cybersécurité n'est pas facultative. Son importance devient évidente lorsqu'une attaque réussie se produit. Mais à ce stade, il est souvent trop tard pour éviter des dommages significatifs. L'adoption d'un cadre de cybersécurité qui applique une approche holistique de ces huit éléments essentiels est susceptible de permettre aux organisations de minimiser les risques et d'éviter des conséquences indésirables.

1 https://www.ft.com/content/728611e8-dce2-449d-bb65-cff11ac2a5bb
2 Données issues de explodingtopics.com en décembre 2023, qui cite Statista comme source d'information. Explodingtopics.com/blog/data-generated-per-day
3 Rapport 2023 d'IBM sur le coût d'une violation de données
4 Données issues de explodingtopics.com en novembre 2023, qui cite Thales Group comme source d'information. Explodingtopics.com/blog/corporate-cloud-data
5 Rapport 2024 sur les menaces mondiales de CrowdStrike.
6 Données d'explodingtopics.com en février 2024, qui cite Transforma Insights comme source d'information. Explodingtopics.com/blog/number-of-iot-devices
7 National Health Executive, octobre 2018. MG fait référence aux médecins généralistes.

Important Risks Related to this Article

INFORMATIONS IMPORTANTES

Communications commerciales publiées dans l¼Espace économique européen (« EEE ») Ce document est publié et approuvé par WisdomTree Ireland Limited, une société autorisée et réglementée par la Central Bank of Ireland.

Communications commerciales émises dans des juridictions en dehors de l¼EEE Ce document est publié et approuvé par WisdomTree UK Limited, une société autorisée et réglementée par la Financial Conduct Authority du Royaume-Uni.

WisdomTree Ireland Limited et WisdomTree UK Limited sont toutes les deux désignées comme « WisdomTree » (le cas échéant). Notre Politique sur les conflits d¼intérêts et notre Inventaire sont disponibles sur demande.

Réservé aux clients professionnels uniquement. La performance passée ne constitue pas une indication fiable des performances futures. Toute donnée de performance historique incluse dans ce document peut avoir été obtenue par calcul a posteriori (« back testing »). Le back testing est le processus qui consiste à évaluer une stratégie d¼investissement en l¼appliquant à des données historiques afin de simuler la performance que cette stratégie aurait produite. La performance ainsi obtenue est purement hypothétique et n¼est fournie dans ce document qu¼à des fins d¼information. Les données obtenues par calcul a posteriori ne représentent pas une performance réelle et ne doivent pas être considérées comme indicatives d¼une performance réelle ou future. La valeur de tout investissement peut être aectée par des fluctuations de taux de change. Toute décision d¼investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d¼investissement, fiscaux et juridiques. Ces produits peuvent ne pas être disponibles sur votre marché ou ne pas vous convenir. Le contenu de ce document ne constitue ni un conseil en investissement, ni une ore de vente ni une sollicitation d¼ore d¼achat d¼un produit ou d¼investissement.

Un investissement dans des produits cotés en bourse (ETP) dépend de la performance de l¼indice sous-jacent, moins les coûts, mais ne doit pas égaler exactement cette performance. Les ETP présentent de nombreux risques, notamment les risques de marché généraux liés à l¼indice sous-jacent concerné, les risques de crédit sur le fournisseur des swaps sur indice utilisés dans les ETP, les risques de change, les risques de taux d¼intérêt, les risques d¼inflation, les risques de liquidité, et les risques juridiques et réglementaires.

Ce document n¼est pas et ne doit en aucun cas être interprété comme, une publicité ou une ore publique de vente d¼actions aux États-Unis ou dans toute province ou tout territoire des États-Unis, où ni les émetteurs ni leurs produits ne sont agréés ou inscrits, où la distribution des produits n¼est pas autorisée et où aucun prospectus des émetteurs n¼a été déposé auprès d¼une quelconque commission des valeurs mobilières ou autorité de règlementation. L¼introduction, la transmission et la distribution (directes ou indirectes) de ce document ou des informations qu¼il contient sont interdites aux États-Unis. Ni les émetteurs ni aucun titre

émis par eux n¼a été ni ne sera enregistré en vertu de la Loi américaine de 1933 sur les valeurs mobilières (United States Securities Act of 1933) ou de la Loi américaine de 1940 sur les sociétés d¼investissement (Investment Company Act of 1940) et aucun d¼eux n¼a été ni ne sera qualifié en vertu des dispositions légales applicables de tout État relatives aux valeurs mobilières.

Ce document peut contenir des commentaires indépendants sur le marché rédigés par WisdomTree sur la base des informations publiques disponibles. Bien que WisdomTree s¼eorce d¼assurer l¼exactitude du contenu de ce document, WisdomTree ne peut en garantir l¼exactitude. Les fournisseurs de données tiers sollicités pour obtenir les informations contenues dans le présent document ne donnent aucune garantie ou représentation de quelque sorte en rapport avec ces données. Lorsque WisdomTree exprime ses propres opinions concernant le produit ou l¼activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses ailiés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l¼utilisation de ce document ou de son contenu.

Ce document peut contenir des déclarations prospectives, y compris notre opinion ou nos attentes actuelles concernant la performance de certains secteurs et/ou catégories d¼actions. Les déclarations prospectives sont sujettes à certains risques, incertitudes et hypothèses. Il n¼existe aucune garantie quant à l¼exactitude de ces déclarations et les résultats réels peuvent diérer sensiblement des résultats prévus dans ces déclarations. WisdomTree recommande fortement de prendre ces déclarations prospectives avec la plus grande précaution.

WisdomTree Issuer ICAV

Les produits pris en considération dans le présent document sont émis par WisdomTree Issuer ICAV (l¼« Émetteur WT »). L¼Émetteur WT est une société d¼investissement à compartiments multiples, à capital variable et à responsabilité séparée entre ses fonds, structurée sous forme de Véhicule de gestion collective d¼actifs de droit irlandais en vertu de la législation irlandaise et agréée par la Central Bank of Ireland (« CBI »). L¼Émetteur WT est structuré sous forme d¼Organisme de placement collectif en valeurs mobilières (« OPCVM ») en vertu de la législation irlandaise et procèdera à l¼émission d¼une catégorie d¼actions distincte (« Actions ») représentative de chaque fonds. Les investisseurs sont invités à lire le prospectus de l¼Émetteur WT (« Prospectus WT ») avant d¼investir, et à consulter la section du Prospectus WT intitulée « Risk Factors » pour plus de détails sur les risques associés à un investissement dans les Actions.

Notice to Investors in Switzerland – Qualified Investors

Le présent document constitue un document promotionnel relatif au(x) produit(s) financier(s) y mentionné(s).

Le prospectus et le Document d¼informations clés aux Investisseurs (DICI) sont disponibles sur le site Internet de WisdomTree : **https:** //www.wisdomtree.eu/fr-ch/resource-library/prospectus-and-regulatory-reports

Certains des compartiments figurant sur le présent document pourraient ne pas avoir été enregistrés auprès de l¼Autorité fédérale suisse de surveillance des marchés financiers (« FINMA »). En Suisse, les compartiments en question, qui n¼ont pas été enregistrés auprès de la FINMA, seront exclusivement distribués à des investisseurs qualifiés, au sens établi par la Loi fédérale suisse sur les placements collectifs de capitaux ou son ordonnance d¼application (chacune pouvant être amendée, le cas échéant). Le représentant et agent payeur des compartiments en Suisse est Société Générale Paris, Zurich Branch, Talacker 50, PO Box 5070, 8021 Zurich, Suisse. Le prospectus, les documents d¼informations clés pour l¼investisseur (DICI), les statuts ainsi que les rapports annuels et semestriels des compartiments sont disponibles gratuitement auprès du représentant et agent payeur. Concernant la distribution en Suisse, le lieu d¼exécution et la juridiction compétente correspondront au siège du représentant et agent payeur.

À l¼intention des investisseurs en France

Les informations présentées dans le présent document sont préparées à la seule intention des investisseurs professionnels (au sens de la directive MiFID) qui investissent pour leur propre compte.

Par ailleurs, ce document ne saurait aucunement être distribué auprès du public. La distribution du Prospectus et l¼ore, la vente ou remise d¼Actions dans d¼autres juridictions peuvent être restreintes ou interdites par la loi. WT Issuer est un OPCVM régi par la législation irlandaise et agréé par la Financial Regulatory (autorité de réglementation financière) en tant qu¼OPCVM conforme à la réglementation européenne, mais n¼est pas tenu néanmoins de respecter les mêmes règles que celles qui s¼appliquent pour un produit similaire agréé en France. Le Fonds a été enregistré à des fins de commercialisation en France par la Financial Markets Authority (Autorité des marchés financiers) et peut être distribué auprès des investisseurs situés en France. Des copies de tous les documents (c¼-à d. le Prospectus, le Document d¼informations clés pour l¼investisseur, tout supplément ou addenda y aérent, les derniers rapports annuels ainsi que l¼Acte et les statuts constitutifs) sont disponibles en France, gratuitement auprès de l¼agent centralisateur français, Societe Generale au 29, Boulevard Haussmann, 75009, Paris, France. Toute souscription d¼Actions du Fonds s¼eectuera selon les conditions prévues dans le prospectus et tout supplément ou addenda y aérent.

For Investors in Monaco

Ce document est destiné spécifiquement et uniquement aux banques dûment enregistrées et / ou les sociétés de gestion de portefeuille autorisées à Monaco. Ce document ne doit pas être envoyée au public à Monaco.