

Un regard militaire sur la cybersécurité (Partie 2)

Publié le 18 mai 2023

Christopher Gannatti, CFA

Global Head of Research

Team8

Global venture group

Dans le premier article de cette série en deux parties, nous avons présenté Nadav Zafir (qui a été commandant de l'Unité 8200, unité d'élite de technologie militaire israélienne, avant de co-fonder Team8) et l'amiral Mike Rogers (qui a terminé sa brillante carrière dans l'US Navy par quatre ans en tant que commandant de l'US Cyber Command et que directeur de la National Security Agency), qui ont partagé leurs points de vue experts sur les quatre premiers des huit thèmes de cybersécurité pour 2023. Dans la deuxième partie, nous allons de nouveau écouter ces experts militaires pendant qu'ils se concentrent sur les quatre thèmes restants.

Thème 5 : Un monde sans périmètre

Nadav Zafir : Dans le monde moderne, axé sur l'informatique dématérialisée et le travail à distance, le périmètre réseau classique a disparu. La pandémie de COVID-19 et le travail à distance généralisé ont accéléré cette tendance, montrant que nos domaines technologiques n'ont plus de limite claire.

Avec la disparition de notre périmètre traditionnel, l'identité est notre nouveau périmètre. Les utilisateurs, les permissions et les points d'accès sont devenus le nouvel intérêt central de la sécurité, et les gérer intelligemment est désormais la clé de la protection de nos organisations.

Les organisations doivent adopter des solutions qui fournissent de la visibilité et du contrôle sur les identités des utilisateurs, notamment le contrôle de l'accès, l'authentification et la gestion des privilèges, qui sont intégrés dans le nuage, sur site et sur le terrain. Ce n'est qu'à cette condition que nous pourrions établir une confiance dans un monde où les limites ont disparu, et assurer que nos ressources et nos informations sont sécurisées tout en étant interconnectées.

Amiral Rogers : Pour moi, nous avons passé 2022 à tenter de comprendre ce qu'était le nouveau normal en termes d'effectifs à distance/hybrides et dans le nouveau monde sans périmètre dans lequel nous vivons. Nous sommes maintenant dans une position où la COVID-19 est quelque chose de durable, sans pics aperiodiques majeurs comme nous avons l'habitude d'en avoir. Avec cela, le modèle de distribution de travail est devenu la norme. À l'avenir, la « dynamique hybride » sera centrale.

Thème 6 : La sécurité des données

Amiral Rogers : Historiquement, les Américains estiment que le gouvernement fédéral doit minimiser son rôle. Ainsi, en ce qui concerne la réglementation de la confidentialité des données, dans l'absence d'une législation fédérale générale, les états ont dû s'impliquer pour combler le manque. Si vous avez une grande entreprise en activité dans de nombreuses géographies nationales, vous ne pouvez pas construire une solution avec 50 exigences en matière de vie privée différentes.

En 2023, nous devons donc évaluer avec précaution ce que le cadre de réglementation américain devrait être pour la protection des données et la confidentialité. Cela se complique encore par le fait qu'aujourd'hui, au Congrès américain, il existe un fort recul en ce qui concerne les grandes entreprises de technologies et de réseaux sociaux. Selon moi, les débats vont continuer sur ces sujets dans les prochains mois et, à l'automne, nous pourrions voir un cadre de nouveaux projets de législation dans le domaine de la protection de la vie privée.

Thème 7 : Un décalage à gauche

Nadav Zafrir : Alors que nous continuons à écrire plus de code que jamais, il devient de plus en plus important d'ajouter de la sécurité à notre processus de développement de logiciels. Cela signifie décaler les pratiques de sécurité pour les intégrer plus tôt dans le processus de développement, ou « décaler à gauche ».

Avec l'utilisation généralisée des logiciels libres, qui constituent la base de nombreuses applications logicielles modernes, et avec l'émergence des développements low-code et no-code, nous approchons rapidement d'un point où tous les membres d'une organisation vont développer et utiliser du code.

Ainsi, il est impératif de s'assurer que chaque membre de l'organisation a une bonne compréhension des pratiques de codage sécurisées et que la sécurité est intégrée dans le processus de développement du logiciel dès le début.

En embrassant une approche de la sécurité plus tôt dans le processus, nous pouvons réduire le risque de vulnérabilité, protéger nos ressources et nos informations et nous assurer que notre logiciel est sécurisé, fiable et résilient.

Amiral Rogers : La chaîne d'approvisionnement est devenue très intéressante, et nous constatons que cette question retient de plus en plus l'attention. Cela a d'abord commencé avec les entreprises privées travaillant avec le gouvernement. Il pourrait cependant y avoir un élan d'expansion des législations des chaînes d'approvisionnement américaines en 2023.

Thème 8 : Layer 8

Nadav Zafrir : Dans le monde de la cybersécurité, l'élément humain est à la fois un atout essentiel et un facteur de risque conséquent. De nombreuses attaques récentes ont pris pour cible des êtres humains de façon encore plus sophistiquée que l'hameçonnage ciblé, qui est très répandu aujourd'hui. Pour répondre à ce défi, nous devons nous concentrer sur la Layer 8, la couche humaine, et construire des outils qui responsabilisent les individus et les aident à prendre de meilleures décisions de sécurité.

Améliorer l'utilisation des outils de sécurité et les rendre intuitifs pour les utilisateurs non techniques est une frontière importante. En permettant aux personnes d'interagir avec la technologie de façon sécurisée et efficace, nous pouvons réduire la probabilité d'erreur humaine menant à des brèches de sécurité.

De la même manière, éduquer les personnes au sujet des meilleures pratiques et les équiper avec les outils et les savoirs leur permettant de prendre des décisions informées est une opportunité de renforcer la posture de sécurité de notre organisation. En fournissant aux employés les bonnes formations et ressources, nous pouvons les transformer en atouts dans la bataille contre les cybermenaces.

Conclusion : suivre les thèmes nous permet de suivre l'évolution de la cybersécurité en cours

L'un des aspects les plus difficiles de l'investissement dans les mégatendances concerne la mesure des progrès. Les mégatendances peuvent être discrètes pendant de longues périodes, et soudain apparaître dans tous les gros titres, comme cela a été le cas pour AI et ChatGPT récemment. Les différents thèmes nous permettent de catégoriser les activités des entreprises et, ainsi, suivre les différents progrès faits en leur sein. Ils aident également à trouver de nouvelles opportunités d'entreprises publiques susceptibles de représenter l'espace au mieux.

Blogs associés

- + [Un regard militaire sur la cybersécurité \(1ère partie\)](#)
- + [La cybersécurité doit demeurer une priorité en 2023](#)
- + [Introducing our newest cybersecurity theme: Layer 8 - The Human Factor](#)

Important Risks Related to this Article

Informations importantes

Communications commerciales publiées dans l'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 l'EEE 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 d'intérêts et notre Inventaire sont disponibles sur demande.

Réservé aux clients professionnels uniquement. Les informations figurant dans ce document sont fournies à titre informatif et ne constituent pas une ore de vente, ou une sollicitation d'ore d'achat de titres ou d'actions. Ce document ne doit pas être utilisé comme fondement d'une décision d'investissement. La valeur des investissements peut fluctuer et vous êtes susceptible de perte tout ou partie du montant investi. La performance passée ne constitue pas nécessairement une indication des performances futures. Toute décision d'investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d'investissement, fiscaux et juridiques.

L'application des réglementations et lois fiscales peut souvent conduire à des interprétations diérentes. Tous les points de vue ou opinions exprimés dans cette communication représentent les points de vue de WisdomTree et ne doivent pas être interprétés comme des conseils réglementaires, fiscaux ou juridiques. WisdomTree ne donne aucune garantie ou représentation quant à l'exactitude des vues ou opinions exprimées dans cette communication. Toute décision d'investissement doit être fondée sur les informations contenues dans le prospectus approprié et après avoir sollicité des conseils indépendants en matière d'investissement, fiscaux et juridiques. Ce document n'est pas et ne doit en aucun cas être interprété comme une publicité ou une ore publique d'actions ou de titres aux États-Unis ou dans toute province ou tout territoire des États-Unis. L'introduction, la transmission et la distribution (directes ou indirectes) de l'original ou d'une copie de ce document sont interdites aux États-Unis.

Bien que WisdomTree s'efforce d'assurer l'exactitude du contenu de ce document, WisdomTree ne peut en garantir l'exactitude. 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 l'activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses alliés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l'utilisation de ce document ou de son contenu.