Un regard militaire sur la cybersécurité (1ère partie)

Publié le 10 mai 2023

Christopher Gannatti, CFA
Global Head of Research

Team8
Global venture group

Bien qu'une interprétation simpliste de la cybersécurité pourrait définir celle-ci comme « la protection des systèmes contre les pirates informatiques », il est important de reconnaître que le sujet est bien plus complexe que cela. Team8 (une société de capital-risque possédant un degré d'expérience exceptionnel dans l'analyse des tendances dans le domaine de la cybersécurité) et WisdomTree ont collaboré afin d'élaborer huit thèmes d'investissement liés à la cybersécurité.

Dans ce blog en deux parties, nous bénéficions du point de vue de Nadav Zafrir et de l'amiral Mike Rogers. Nadav Zafrir a été commandant de l'unité 8200, l'unité technologique militaire d'élite israélienne, avant de co-fonder Team8. La brillante carrière de l'amiral Rogers dans la marine de guerre américaine a connu son apogée avec une mission de quatre ans en tant que commandant de l'US Cyber Command et directeur de la National Security Agency. Mises bout-à-bout, leurs expériences et leurs réussites nous offrent une expertise des plus pointues issue des deux pays les plus influents en matière de cybersécurité. Découvrons leur point de vue sur les quatre premiers de nos huit thèmes liés à la cybersécurité.

Thème 1 : Sécurité du cloud

Nadav Zafrir : Alors que nous composons avec une migration vers le cloud en pleine accélération, nous devons reconnaître que, bien qu'il présente de nouveaux défis de sécurité en raison de sa flexibilité, le cloud offre également des opportunités uniques en la matière. Les données circulent vers de nouveaux partenaires et services, tandis que le réseau est simplifié et plus facilement identifiable pour les cyber-criminels. Tout est cependant visible et nous possédons une connaissance plus approfondie que jamais de nos systèmes, ainsi que de tout ce qu'il s'y passe.

Avec l'essor à venir de l'intelligence artificielle (IA), la migration vers le cloud ne sera plus simplement nécessaire, mais impérative pour les organisations de premier plan. Dans le monde multi-cloud plus SaaS (logiciel en tant que service) dans lequel nous vivons, avec des opérateurs de cloud résolvant une partie de l'équation et des services natifs cloud de plus en plus performants, agir en toute sécurité dans le cloud est essentiel pour la quasi-totalité des entreprises.

Amiral Rogers : Au fur et à mesure que les cibles (les entreprises) commencent à déplacer une grande partie de leurs données dans le cloud, nous allons voir les acteurs des États-nations se focaliser principalement sur les concentrations de données dans le cloud.

Thème 2 : Résilience et rétablissement

Nadav Zafrir : Un ransomware est un type d'attaque sophistiqué et motivé par l'argent de plus en plus fréquent ces dernières années. En effet, les cybercriminels utilisent des méthodes toujours plus sophistiquées pour infiltrer les réseaux organisationnels, d'autant plus qu'ils sont, dans de nombreux cas, aujourd'hui soutenus par des gouvernements. Par conséquent, les organisations doivent faire preuve d'initiative dans leur approche de la sécurité, en étant conscientes que la question n'est pas de savoir si, mais quand elles devront affronter une attaque par ransomware.

Pour lutter efficacement contre cette menace, les organisations sont en train de réorienter leur efforts pour ne plus simplement essayer d'empêcher les attaques, mais également pour se préparer à l'inéluctabilité d'une attaque réussie. Cela implique l'élaboration d'une stratégie de sécurité exhaustive qui inclut non seulement des contrôles techniques permettant de détecter et d'empêcher les attaques, mais également des politiques, des procédures et des formations clairement définies pour permettre un fonctionnement ininterrompu et un rétablissement rapide. En adoptant cette approche, les organisations peuvent améliorer leur résilience en cas d'attaque et garantir un rétablissement sans délai, tout en poursuivant leurs activités essentielles.

Amiral Rogers : Le nombre d'attaques par ransomware restera plus important dans certains secteurs précis que dans d'autres, comme par exemple le secteur de la santé/des infrastructures essentielles, etc. C'est pourquoi l'accent est mis sur « la résilience, la résilience et la résilience », qui continuera à gagner de l'importance en 2023. Ce problème sera exacerbé, surtout en cas de diminution des budgets et de pénurie de main-d'œuvre, car les entreprises rechercheront l'efficacité partout où ils pourront la trouver.

Bien que les attaques par ransomware soient habituellement une question d'accès, nous allons également observer une augmentation du « facteur honte » afin d'inciter les victimes à payer des rançons plus importantes. Même si la plupart des entreprises ne l'admettront pas, le nombre d'entreprises payant la rançon diminue progressivement. Quelle est la réaction des criminels ? Les pirates informatiques ont besoin de découvrir quelles autres raisons motiveront l'entreprise à payer, comme par exemple une humiliation publique et le risque lié à la réputation/l'atteinte à l'image.

Thème 3 : Une sécurité plus intelligente

Nadav Zafrir : Dans le paysage complexe et en constante évolution des menaces d'aujourd'hui, le nombre de services et d'applications est plus élevé que jamais, mais le nombre de professionnels de la sécurité pour les protéger n'évolue pas. Dans le même temps, les attaques sont devenues plus rapides et plus sophistiquées, ce qui rend le rythme plus compliqué à suivre pour les entreprises.

Pour remédier à cela, les organisations exigent désormais des outils de sécurité plus intelligents qui s'intègrent à d'autres technologies, possèdent des interfaces de programmation d'application (API) pour

plus de personnalisation et offrent des recommandations intelligentes. Une sécurité plus intelligente implique également l'utilisation d'outils d'analyse avancés et d'une cyberveille afin d'identifier et de faire face à d'éventuelles cybermenaces efficacement et dans les meilleurs délais. En se concentrant sur ce qui est réellement important et en investissant dans les technologies et mesures de sécurité adéquates, les organisations peuvent améliorer leur stratégie de sécurité et réduire le risque de cyberattaques.

Cette tendance vers une sécurité plus intelligente ne fera que s'accélérer au cours des années à venir. Alors que nous tentons de gérer cette complexité croissante, nous devons tirer parti des nouvelles technologies telles que l'IA pour nous aider à garder une longueur d'avance.

Amiral Rogers : L'une des dynamiques que j'anticipe pour les responsables de la sécurité des systèmes d'information (RSSI) est que la plupart d'entre eux ont généralement profité de 5 à 7 années de croissance continue, avec notamment des augmentations annuelles du budget et de la main-d'œuvre. Cependant, de très nombreuses entreprises font aujourd'hui face à une éventuelle récession et à un contexte économique difficile. Les gens se font licencier à tout-va.

À l'avenir, certains PDG pourront penser que la croissance continue de l'informatique n'est pas durable et qu'ils ne peuvent tout simplement pas continuer à accorder 15 % de rallonge budgétaire aux RSSI chaque année. Nous devrons nous forcer à demander à quoi ressemble un modèle plus efficace et aux ressources plus limitées ? C'est là qu'intervient la sécurité plus intelligente.

Thème 4 : La sécurité des objets

Nadav Zafrir : Au fur et à mesure que le nombre d'appareils connectés continue d'exploser, ceux-ci s'intègrent de plus en plus à nos vies et sont, bien souvent, en mesure d'influer sur l'espace physique qui nous entoure.

Même si la plus-value apportée par les appareils connectés est évidente, ces derniers peuvent également nous exposer à de nouveaux et dangereux vecteurs d'attaques. C'est la raison pour laquelle la mise en place d'une sécurité évolutive pour ces appareils est d'une importance capitale, en particulier en ce qui concerne les technologies émergentes telles que les drones, les voitures connectées, les dispositifs médicaux connectés ou les usines intelligentes, entre autres, qui peuvent toutes influer sur le monde réel et mettre des vies en danger.

Pour ce faire, les organisations et les prestataires doivent développer des outils et des stratégies de sécurité qui tiennent compte des défis et des risques uniques que présente la sécurité des objets. Cela exige une collaboration entre les fabricants, les organismes de réglementation et les experts en sécurité afin de créer des normes, des structures d'encadrement et des pratiques de références liées à la sécurisation de ces appareils tout au long de leur cycle de vie.

Amiral Rogers : Je m'attends à ce que l'accent soit davantage mis sur la technologie opérationnelle (TO) et sur l'Internet des objets (IdO), en particulier sur la fonctionnalité, et non uniquement sur les données. On peut s'attendre à ce que les cybercriminels approchent les infrastructures essentielles d'une façon

plus analytique. En d'autres termes, ils ne se diront plus : « Attaquons-nous à la compagnie des eaux X et voyons si nous pouvons pénétrer leur réseau. »

Ils étudieront plutôt leurs cibles de façon plus globale, en analysant leurs réseaux, structures de fonctionnement, accès à distance, vulnérabilités dans les systèmes intégrés et de base, chaînes d'approvisionnement, etc. afin d'identifier le chemin le plus efficace pour atteindre leur objectif.

Ne manquez pas la 2e partie, dans laquelle nous aborderons les 4 autres thèmes : un monde sans périmètre, la sécurité des données, la stratégie « shift-left » et notre nouveau thème, la couche 8.

Blogs associés

+ 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 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. Les informations figurant dans ce document sont fournies à titre informatif et ne constituent pas une ore de vente, ou une sollicitation d¼ore d¼achat de titres ou d¼actions. Ce document ne doit pas être utilisé comme fondement d¼une décision d¼investissement. 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 d¼investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d¼investissement, fiscaux et juridiques.

L¼application 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 n¼est pas et ne doit en aucun cas être interprété comme une publicité ou une ore publique d¼actions ou de titres aux États-Unis ou dans toute province ou tout territoire des États-Unis. L¼introduction, la transmission et la distribution (directes ou indirectes) de l¼original ou d¼une copie de ce document sont interdites aux États-Unis.

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.