La cybersécurité protège les données et l'intégrité des ressources informatiques connectées ou installées sur un réseau d'entreprise. Elle a pour mission de défendre ces ressources contre tous les pirates, et ce tout au long du cycle d'attaque.

Les tournants ont eu lieu « en 2007/2008, quand les entreprises qui ont multiplié les projets d'informatisation et de mise en réseau ont réalisé leurs nouvelles vulnérabilités », dit un expert en cybersécurité du cabinet Wavestone.

Depuis 2011, les premières méga cyberattaques ont éclairé sur l'importance d'investir dans ce segment. Un des évènements marquants : Le piratage de Sony Pictures Entertainment en 2014. Les employés de la société ont vu apparaitre un message de menace de pirates leur réclamant de l'argent sous 24h sinon leurs données seraient dévoilées. Ainsi, 5 films de la firme japonaise ont finalement été révéléss sur internet causant un préjudice estimé à 100 millions de dollars.

Depuis, le coût direct mondial de la cybercriminalité a beaucoup augmenté et est aujourd'hui estimé à plus de 400 milliards de dollars par an. Cette dynamique encourage les pirates informatiques à poursuivre leurs activités et entraîne un fort accroissement des dépenses de sécurité visant à contrer de nouvelles menaces.

Face à l'évolution quotidienne des attaques et à l'inventivité croissante des pirates, il est désormais primordial pour les sociétés d'avoir un plan précis et d'identifier les éléments clés de leur cybersécurité.

Ce secteur est d'autant plus renforcé depuis l'apparition de la crise sanitaire. Les cyberattaques se sont multipliées durant cette période, notamment à cause du développement du télétravail qui a fragilisé les infrastructures informatiques des entreprises.

De ce fait, ce marché pèse 150 mds$ en 2021 d'après la dernière estimation de Gartner, entreprise américaine de conseil et recherches. Le taux de croissance annuel dépasserait les 12%, soit quasiment le double de celui enregistré en 2020. Cette croissance est principalement dûe au fait que la cybersécurité ressort comme l'un des principaux postes de dépenses priorisés par les dirigeants.

Selon des chiffres rapportés par PWC, la dernière décennie a vu émerger une

vingtaine de « licornes » (start-up valorisées plus d'un milliard de dollars) dont une dizaine rien que dans les deux dernières années.

Bien que petite par sa taille, la France est un poids lourd de la cybersécurité dans le monde avec des acteurs de poids. On y retrouve Airbus Cybersecurity qui occupe la place de leader sur le marché européen et mondial dans la protection informatique, Thales qui est mondialement connu pour son travail sur le programme GALILEO (système de géolocalisation par satellite), Safran, Orange Cyberdéfense et Capgemini.

Finalement, ça correspond à quoi la cybersécurité ?

La cybersécurité consiste à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les attaques malveillantes. Elle est divisée en plusieurs catégories :

- La **sécurité réseaux** consiste à protéger le réseau informatique contre les intrus, qu'il s'agisse d'attaques ciblées ou de malwares opportunistes.
- La **sécurité des applications** vise à protéger les logiciels et les appareils contre les menaces. Une application corrompue pourrait ouvrir l'accès aux données qu'elle est censée protéger. Un système de sécurité fiable se reconnaît dès l'étape de conception, bien avant le déploiement d'un programme ou d'un appareil.
- La **sécurité des informations** veille à garantir l'intégrité et la confidentialité des données, qu'elles soient stockées ou en transit.
- La **sécurité opérationnelle** comprend les processus et les décisions liés au traitement et à la protection des données. Les autorisations des utilisateurs pour l'accès au réseau et les procédures qui définissent le stockage et l'emplacement des données relèvent de ce type de sécurité.
- La **reprise après sinistre et la continuité des opérations** spécifient la manière dont une entreprise répond à un incident de cybersécurité ou tout autre événement causant une perte des opérations ou de données. Les politiques de reprise après sinistre régissent la manière dont une entreprise recouvre ses opérations et ses informations pour retrouver la même capacité de fonctionnement qu'avant l'événement. La continuité des opérations se réfère au plan sur lequel s'appuie une entreprise tout en essayant de fonctionner sans certaines ressources.
- La **formation des utilisateurs** finaux porte sur le facteur le plus

imprévisible : les personnes. Tout le monde peut accidentellement introduire un virus dans un système habituellement sécurisé en ne respectant pas les bonnes pratiques de sécurité. Apprendre aux utilisateurs à supprimer les pièces jointes suspectes et à ne pas brancher de clés USB non identifiées est essentiel pour la sécurité d'une entreprise.

Focus entreprises : Zscaler

Zscaler est une société américaine de sécurité de l'information basée sur le cloud dont le siège social est situé à San Jose, en Californie. En novembre 2021, l'entreprise avait une capitalisation boursière de plus de 45 milliards de dollars américains. L'entreprise possède plus de 150 centres de données avec des clients dans 185 pays. Ils sont majoritairement situés aux États-Unis, et la plupart d'entre eux comptent plus de 10 000 employés.

Zscaler a été fondée en 2007 par Jay Chaudhry et K. Kailash. Elle a fait une introduction en bourse en mars 2018, où elle a levé 192 millions de dollars. La société a généré 673 millions de dollars de revenus bruts pour l'année fiscale 2021. Avec l'apparition croissante du cloud, Zscaler a décidé d'acheter la startup de protection de données dans le cloud, Cloudneeti.

Zscaler définit la cybersécurité comme la combinaison de personnes, de politiques, de processus et de technologies visant à protéger les réseaux, les dispositifs et les données contre tout accès non autorisé ou toute utilisation criminelle et la pratique consistant à garantir la confidentialité, l'intégrité et la disponibilité des informations.

Article rédigé par Alioune Niang et Yohann Derbyshire.