Cyberattaques menées par un État : une menace majeure pour les entreprises

La majorité des entreprises interrogées dans le cadre d'une étude menée par l'*Economist Intelligence Unit* (EIU) et le *Cybersecurity Tech Accord* publié ce jour considère les cyberattaques commanditées par un État comme une menace de premier plan pour leurs activités. Ces entreprises s'inquiètent des conséquences réputationnelles et financières qui découlent de ces attaques et appellent à une plus grande coopération politique internationale afin de faire face à ces menaces.

Cette étude a été menée entre novembre et décembre 2020, avant que la cyberattaque contre la société de logiciels *SolarWinds* ne soit révélée. Cette attaque a poussé de de nombreuses organisations à réfléchir aux défis posés par les cyberattaques commanditées par un État. Cependant, comme le révèle l'étude, de nombreuses entreprises sont depuis longtemps conscientes de la montée en puissance de ce type d'attaque.

Ces dernières années, les cyberattaques perpétrées par des États ont transformé le cyberespace. Cette escalade du conflit en ligne a été accélérée par la COVID-19. Près de 8 personnes interrogées sur 10 affirment que la pandémie a augmenté la probabilité d'une cyberattaque menée par un État contre l'organisation dans laquelle elles travaillent.

Comme le révèle l'étude, les dirigeants du secteur privé s'attendent à ce que les cybermenaces émanant d'acteurs étatiques augmentent dans les années à venir et souhaitent que les gouvernements prennent des mesures afin de mettre en œuvre des solutions efficaces au niveau national et international pour les contrer. Les principaux résultats de l'étude sont présentés plus en détail ci-dessous :

- **Les cyberattaques menées par un État sont une source d'inquiétude croissance pour les entreprises.** 80 % des personnes interrogées se disent inquiètes face au risque que leur organisation soit victime d'une cyberattaque menée par un État. La majorité des interrogés déclarent que cette inquiétude s'est accrue au cours des cinq dernières années.
- **Les entreprises s'attendent à ce que les cyberattaques émanant d'acteurs étatiques augmentent dans les cinq prochaines années.** Les personnes interrogées s'attendent à ce que, dans cinq ans, la menace venant des États soit la deuxième plus importante après celle du crime organisé. Il s'agirait d'une évolution majeure étant donné que les États disposent de ressources importantes et d'outils et technologies de pointe, pouvant être réutilisés par d'autres agresseurs.
- **Il existe un sentiment de sécurité infondé.** 68 % des cadres d'entreprises interrogés estiment que leur organisation est « très » ou « complètement » préparée à faire face à une cyberattaque. Or, Charles Carmakal, vice-président et directeur de la technologie chez *FireEye*, interrogé par l'EIU, suggère qu'en réalité, la plupart des organisations n'ont pas l'expérience requise pour faire face à de telles menaces, car elles sont rarement les premières cibles de ces attaques. Le récente attaque envers *SolarWinds* pourrait obliger davantage d'organisations à réfléchir à la manière dont elles peuvent limiter ces risques.

- **L'augmentation des investissements des entreprises dans la cybersécurité est essentielle et l'action gouvernementale, au niveau national et international, primordiale.** Six dirigeants d'entreprises sur dix affirment que leur pays n'offre qu'un niveau de protection moyen ou faible et qu'une coopération économique et politique internationale plus forte est primordiale pour faire face à ces menaces et cultiver un environnement en ligne plus sûr et plus stable.

« Les attaques dirigées par un État sont le signal de l'aggravation d'un problème trop important pour être ignoré », a déclaré Brad Maiorino, vice-président exécutif et directeur de la stratégie, FireEye. « Il faut un changement fondamental dans la gestion et la conception de la sécurité, au-delà des efforts d'une seule organisation, et ce changement nécessite une action proactive et coopérative de la part des gouvernements et de l'industrie ».

« Bien que les cyberattaques soient une menace discrète, elles peuvent avoir des effets dévastateurs et durables sur notre société. Compte tenu de la récente escalade des tensions dans le cyberespace, la coopération entre les gouvernements devient de plus en plus compliquée, car les systèmes politiques diffèrent et la concurrence technologique s'intensifie », a déclaré Marietje Schaake, présidente du *CyberPeace Institute*. « Cette étude est un appel à l'action afin que les gouvernements démocratiques s'engagent et réfléchissent plus largement au type de cyberassistance qu'ils doivent fournir pour protéger les entreprises dans des secteurs clés, et en fin de compte, les citoyens ».

Depuis sa création, le *Cybersecurity Tech Accord* met en lumière cette situation préoccupante et invite les gouvernements à protéger le cyberespace et à s'abstenir d'utiliser l'Internet comme terrain de conflit, directement ou par l'intermédiaire de tiers. En tant que porte-parole de l'industrie et ardent défenseur d'un comportement responsable dans le cyberespace, le *Cybersecurity Tech Accord* a constamment appelé les gouvernements à faire plus pour se dresser contre les menaces en ligne, à faire respecter le droit international et à mettre en œuvre les normes internationales de cybersécurité.

« En tant que coalition de plus de 150 entreprises mondiales du domaine de l'information et des nouvelles technologies, nous sommes très préoccupés par les cyberattaques menées par des forces étatiques, qui sont de plus en plus fréquentes et sophistiquées. Il faut agir, et vite », a déclaré Annalaura Gallo, membre du secrétariat du *Cybersecurity Tech Accord*. « Cette étude montre que les entreprises considèrent les cyberattaques lancées par les États comme une problématique urgente qui exige des gouvernements qu'ils agissent au niveau national et international. Nous avons besoin d'un accord aux Nations Unies et de la participation des entreprises et de la société civile, notamment par le biais de forums multipartites tels que l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Nous espérons que les résultats de cette étude seront le point de départ d'une conversation plus globale sur ce sujet essentiel ».

L'étude a été menée auprès de plus de 500 dirigeants de niveau directeur ou supérieur d'Asie-Pacifique, d'Europe et des États-Unis, tous familiarisés avec la stratégie cybersécurité de leur organisation. Ils représentant un large éventail de secteurs, à commencer par l'informatique et les nouvelles technologies, le commerce de détail ou encore la production de biens de consommation.

Pour un résumé des principales conclusions du rapport, voir l'infographie ici, et pour les

informations détaillées, lire le document ici.

Pour en savoir plus sur le *Cybersecurity Tech Accord*, rendez-vous sur www.cybertechaccord.org.

À propos du Cybersecurity Tech Accord : En avril 2018, 34 entreprises mondiales des secteurs des nouvelles technologies et de la sécurité ont signé le *Cybersecurity Tech Accord*, un accord déterminant et un engagement public pour protéger et responsabiliser les civils en ligne. Depuis, cette initiative est devenue le plus grand effort industriel de ce type, avec plus de 150 entreprises signataires dans le monde entier qui s'engagent à améliorer la sécurité, la stabilité et la résilience du cyberespace. Pour plus d'informations, rendez-vous ici.

A propos de l'Economist Intelligence Unit (EIU) : L'EIU est la division en charge de la recherche et de l'analyse de *The Economist Group* et le leader de l'intelligence économique mondiale pour les dirigeants. L'EIU offre des prospectives innovantes grâce au travail de plus de 650 analystes et rédacteurs experts dans 200 pays du monde entier. Pour plus d'informations, rendez-vous ici.