Deloitte.

L’affaire SolarWinds sonne l’alarme : pourquoi le moment est venu de s’attaquer aux risques de concentration

La semaine dernière, une foule d’organismes gouvernementaux de haut niveau et de grandes entreprises de partout en Amérique du Nord, en Europe, en Asie et au Moyen-Orient ont été ébranlés par la nouvelle que leurs réseaux pourraient avoir été exposés par un État présumé être derrière une attaque.

SolarWinds, une entreprise de logiciels qui compte plus de 300 000 clients, a avisé que 18 000 d’entre eux avaient pu télécharger un produit phare possiblement infecté par un code malveillant permettant aux pirates d’accéder à leurs systèmes par des moyens détournés.

Devant le peu d’information accessible à la fois sur les répercussions et sur l’étendue de l’attaque, les dirigeants d’entreprise et les chefs de la sécurité de l’information subissent des pressions – que leur organisation ait été directement touchée ou pas. Les conseils d’administration, les clients, les fournisseurs et même le marché exigent d’être immédiatement informés de l’ampleur du problème.

Un problème généralisé et pernicieux

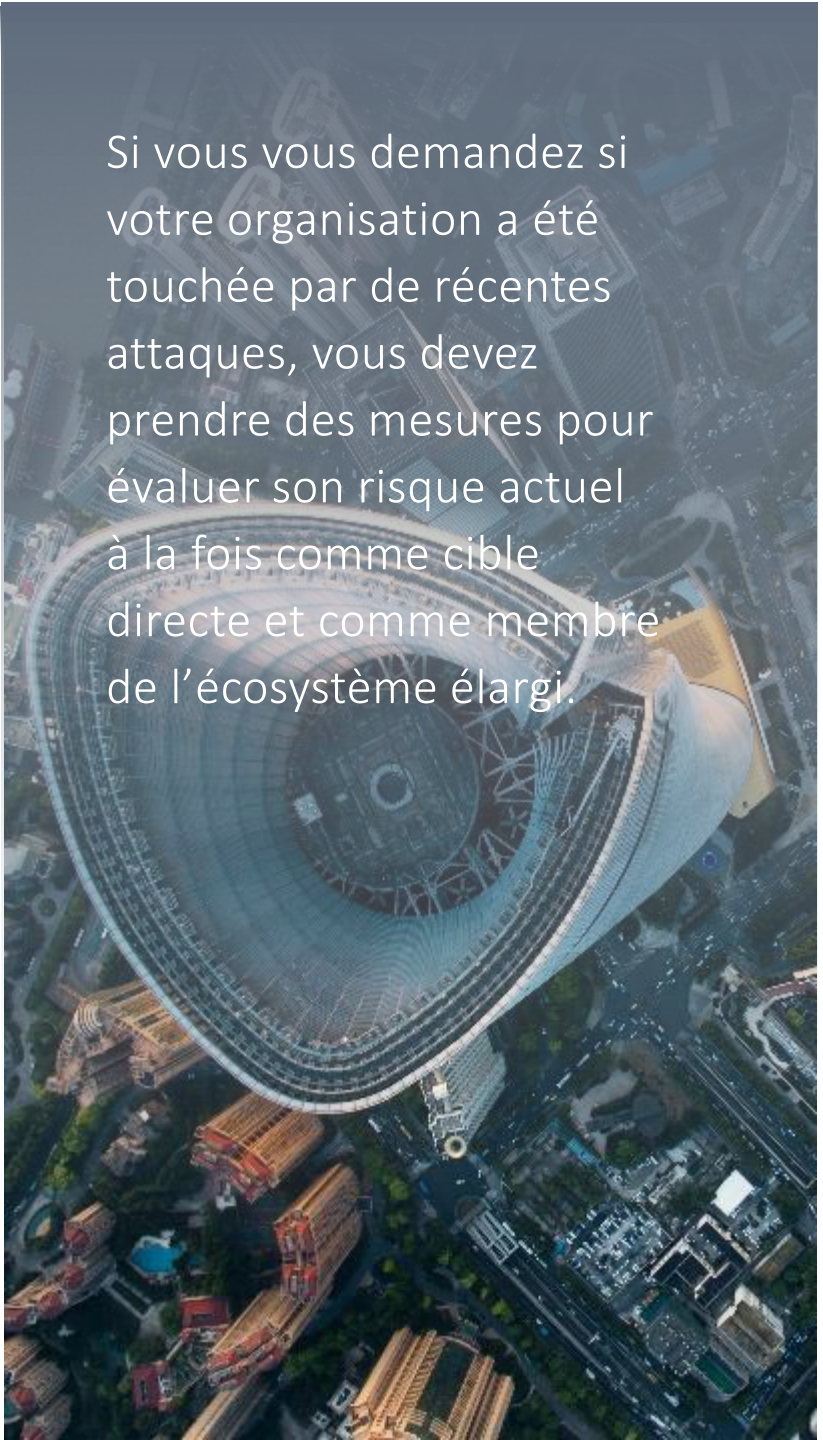
L’une des raisons pour lesquelles les organisations vont vers les meilleures solutions technologiques est la sécurité inhérente qu’elles leur procurent manifestement. Les fournisseurs réputés d’outils de détection et d’intervention sur les points de terminaison (EDR), de solutions d’infrastructure infonuagique et de services de sécurité gérés ont acquis à juste titre un statut de confiance dans la plupart des organisations. Ces entreprises sont les plus sérieuses au sujet de la mise en œuvre d’infrastructures de sécurité inattaquables.

Grâce à leurs capacités de haut niveau, ces tiers fournisseurs finissent généralement par servir des dizaines de milliers de clients de multiples secteurs et régions, ouvrant ainsi la porte au risque de concentration.

Généralement défini comme la probabilité de pertes pouvant survenir en raison de la trop grande dépendance à un fournisseur unique, le risque de concentration est aggravé quand le fournisseur en question se spécialise dans un secteur donné. Plus ces entreprises ont une bonne réputation, plus il est probable qu’elles aient un accès privilégié à des réseaux qui hébergent des renseignements extrêmement confidentiels et souvent classifiés. Elles font partie de la structure et on leur fait naturellement confiance, ce qui en fait des cibles particulièrement attrayantes pour les auteurs de menaces sophistiquées.

La dure réalité est que les attaques de ce genre sont plus fréquentes qu’on le pense. Les cybercriminels et les groupes de menaces persistantes évoluées ciblent sans relâche même les environnements les plus sécurisés. Malgré le seuil plus élevé, le piratage de ces environnements leur procure des avantages considérables : plutôt que de s’introduire dans un ou plusieurs systèmes dorsaux, ils peuvent ainsi s’infiltrer dans tout un secteur ou toute une région.

En période de pandémie, les nombreuses attaques par des rançongiciels, les vols de données hautement médiatisés ou les craintes d’atteinte à la sécurité de systèmes à distance font souvent les manchettes. Bien sûr, les chefs de la sécurité de l’information et leurs équipes accordent la priorité à leurs ressources.



Aucune organisation n'est à l'abri d'une atteinte à la cybersécurité

Les organisations sont nombreuses à identifier des risques de concentration potentiels, mais la plupart reportent le moment de s'y attaquer. Qui aurait pu penser qu'un fournisseur mondial de confiance ou que la meilleure solution du secteur deviendrait un vecteur d'attaque réel?

En attendant, les auteurs de menaces comprennent l'importance de prendre le contrôle de fournisseurs de confiance ou de leurs solutions. Dans la mesure du possible, leurs travaux sont secrets et hautement spécialisés. Lorsqu'ils réussissent une attaque contre un fournisseur d'infrastructure, ils peuvent toucher un rendement sur leur investissement à plusieurs reprises, dans de nombreux secteurs et régions.

Comprendre les conséquences

Quand il s'agit de faire la chronique des répercussions des atteintes à la cybersécurité, ce ne sont pas les statistiques qui manquent. Selon le cabinet spécialisé en recherches Cybersecurity Ventures, le coût de la cybercriminalité à l'échelle mondiale atteindra 10,5 billions de dollars d'ici 2025, une somme qui dépasse largement ce que coûtent les dommages causés annuellement par les catastrophes naturelles[1].

Cette information cache cependant d'innombrables répercussions, allant de la destruction de données, des pertes financières ainsi que du vol de propriété intellectuelle et de renseignements permettant d'identifier des personnes, à la perturbation des activités, des pertes d'emplois et souvent une atteinte irréversible à la réputation. Malgré ce lourd bilan, pourtant, les chiffres ne révèlent pas tout.

En fait, ces attaques sont les plus dévastatrices lorsque les organisations ne peuvent évaluer ce qu'elles leur coûtent, simplement parce qu'elles ne savent même pas qu'elles en sont des victimes. Certaines variantes de logiciels malveillants sont si avancées qu'elles peuvent rester inactives dans un système pendant des jours ou des semaines, ce qui les rend presque impossibles à détecter.

Une fois libérés, un grand nombre de ces fichiers malveillants se répandent dans l'ensemble du réseau de l'organisation, donnant aux pirates un accès continu aux systèmes de la cible même après que la porte dérobée initiale est désactivée. Souvent, les organisations ne se rendront même pas compte de l'intrusion avant plusieurs mois, voire des années.

Réagir intelligemment

Si vous vous demandez si votre organisation a été touchée par de récentes attaques, vous devez prendre des mesures pour évaluer son risque actuel à la fois comme cible directe et comme membre de l'écosystème élargi. Avant de pouvoir répondre aux dirigeants responsables, vous devez déterminer si vous ou d'autres membres de votre écosystème avez été mis en danger, préciser ce que vous jugez être la surface d'attaque et déterminer les points d'accès potentiels.

Bien que vous puissiez être tenté d'entreprendre immédiatement des efforts visant à contenir l'incident, il est souvent nécessaire de prendre du recul et d'évaluer d'abord l'ampleur de l'intrusion. En dévoilant votre jeu trop rapidement, vous pourriez perdre le levier dont vous disposez pour assurer un rétablissement complet.

Si votre organisation dispose d'un guide d'intervention en cas de crise, vous êtes sans doute bien placé pour définir les prochaines étapes. Si vous n'avez pas de guide, par contre, vous devrez réfléchir aux mesures à prendre alors que vous êtes sous pression, sans doute en collaboration avec les avocats, l'assureur et le coach en matière d'atteintes à la protection des données de l'organisation.

Il est par ailleurs intéressant de souligner que même les organisations qui sont intouchées ne le sont pas réellement. L'attaque de la dernière semaine a une fois de plus montré qu'aucune organisation n'est à l'abri d'une atteinte à la cybersécurité. C'est là un vif rappel de la nécessité de toujours renforcer l'hygiène de base en matière de cybersécurité afin de minimiser les répercussions du risque de concentration.

Certaines organisations pourraient devoir se pencher sur leurs responsabilités et leurs obligations envers des tiers. Pour d'autres, il pourrait être nécessaire de catégoriser les fournisseurs d'intérêts particuliers et d'évaluer où elles se situent dans l'écosystème élargi des fournisseurs. Individuellement, il ne faut pas oublier que cela nous concerne tous. En renforçant collectivement nos positions en matière de cybersécurité, nous pouvons non seulement accroître la résilience organisationnelle, mais également rehausser le niveau de cybermaturité partout.

I. Morgan, Steve. « *Cybercrime To Cost The World $10.5 Trillion Annually By 2025* », *Cybercrime Magazine*, 13 novembre 2020, https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016.

Si vous subissez des pressions pour minimiser l'incidence d'un cyberincident en cours, si vous souhaitez connaître les options qui s'offrent à vous pour gérer les risques de concentration ou si vous voulez simplement améliorer votre préparation à faire face aux menaces futures, communiquez avec les Services de cybersécurité de Deloitte.

Auteurs et personnes-ressources

Amir Belkhelladi | Leader de la cybersécurité, Canada
abelkhelladi@deloitte.ca

Rob Masse | Leader de la cybersécurité infonuagique, Amérique du Nord
rmasse@deloitte.ca