HISCOX
CYBERCLEAR®

LES CINQ PRINCIPAUX CYBER-RISQUES EN 2021

Les cyber-risques dans le monde ont rapidement évolué au cours de l'année 2020, et concernent des entreprises de toutes tailles et dans tous les secteurs. L'impact de la pandémie de COVID-19 s'est fait ressentir par un nombre accru de victimes d'emails de phishing au mois de mars. Néanmoins, elle a également eu pour effet d'accentuer la sensibilisation aux cyber-risques des consommateurs et des entreprises.

A la fin de l'année 2019, on a vu pour la première fois des groupes de pirates diffusant des ransomware menacer de publier des données qu'ils avaient volées. Cette évolution des ransomware vers la divulgation (*doxing*) ou la publication de données volées signifie que les attaques par ransomware constituent désormais des failles de données. Dorénavant, les coûts seront plus élevés et il sera plus long de se remettre de ces attaques. Les actions en justice se sont multipliées aux Etats-Unis et au Royaume-Uni en raison de la prolifération des failles de données, principalement dues aux piratages de comptes de messagerie électronique professionnelle et aux ransomware/divulgations de données.

Les ports RDP (*remote desktop protocol*) ouverts, l'absence de correctifs et les vulnérabilités des réseaux privés virtuels (VPN) ont représenté les causes principales des ransomware en 2020. Au cours de l'été, Microsoft a publié plus d'une centaine de vulnérabilités par mois, nécessitant un effort important de correction de failles pouvant rendre les entreprises vulnérables.

Au cours de l'automne et de l'hiver, des failles de la chaine logistique de grande ampleur, à savoir Blackbaud et SolarWinds, ont fait la une des journaux. Elles ont en effet impacté des entreprises internationales et presque tous les départements du gouvernement américain. La portée de ces deux attaques continue de s'étendre.

Alors que faire ? Le grand enseignement de 2020 est qu'il est primordial que les entreprises prennent la cybersécurité au sérieux. Certaines menaces vont perdurer et les entreprises de toutes tailles doivent se protéger, rester vigilantes et renforcer leur résilience.

Persistance de la menace liée au COVID-19
Les campagnes de phishing qui s'appuyaient sur la diffusion de données liées au COVID-19, cibleront désormais les informations liées au vaccin et l'inscription à la vaccination. Les attaques vont probablement porter sur les efforts de lutte contre le COVID-19 et les services et secteurs concernés, notamment la santé, les services locaux de l'Etat, les distributeurs de vaccins etc.

Evolution des ransomware
Les cybercriminels sont créatifs et innovants lorsqu'il s'agit de faire pression pour que leurs victimes paient. Différents vecteurs d'attaque seront utilisés simultanément pour provoquer de plus grandes perturbations, les attaques par déni de service et divulgations de données en plus des ransomware. Les ports RDP ouverts et les vulnérabilités des accès à distance continueront d'être les points d'entrée principaux des cybercriminels. La divulgation de données peut entrainer des frais importants pour toutes les entreprises et pour l'ensemble des acteurs de la cyber-assurance.

Transformation du paysage juridique
Les actions de tiers et recours collectifs, tout comme les amendes réglementaires ou celles fondées sur le RGPD se multiplieront à mesure que les failles de données prendront de l'ampleur, en raison des divulgations de données et attaques de la chaine logistique. L'accentuation de la menace liée aux ransomware va pousser les gouvernements à réagir et entrainer une modification des politiques relatives aux paiements de rançons et aux exigences de prévention.

Répercussions de SolarWinds
Ses impacts immédiats et ramifications étendues sont toujours inconnus. Il est probable que les chaines logistiques de logiciels soient la cible d'attaques par imitation (*copycat attacks*). Les services d'établissement et de déploiement ont toujours été conçus selon des critères de rapidité et de commodité et non à des fins de sécurité. Méfiez-vous de l'exploitation des vulnérabilités critiques de Microsoft et d'autres fournisseurs de services numériques.

Nouveaux vecteurs d'attaque
Nous devons faire preuve de la même créativité que les cybercriminels et anticiper leurs actions. Il conviendrait de surveiller en particulier les malware ciblant les terminaux de vente, les orages magnétiques et autres armes électromagnétiques, les attaques des protocoles de synchronisation des heures (*time protocols*) et les kits d'exploitation malveillants (*weaponized exploit kits*).