Cybersécurité

Une menace sous-estimée

Le risque informatique est devenu la première menace pour les entreprises du monde entier. Particulièrement exposés, les laboratoires pharmaceutiques doivent impérativement s'emparer du sujet. La problématique soulève des enjeux techniques, humains, organisationnels et financiers.

Selon IBM Security, le coût total d'un vol de données dans le secteur de la santé est estimé à 7,13 millions de dollars, en moyenne.

© Adobestock

La nouvelle a fait grand bruit. L'Agence européenne du médicament a été victime d'une cyberattaque le 9 décembre dernier. Les pirates informatiques ciblaient visiblement le vaccin co-développé par Pfizer et BioNTech. D'après les premières constations, les données personnelles des participants aux essais cliniques ne semblaient pas avoir été altérées. Certains documents confidentiels, en lien avec la demande d'autorisation en cours d'examen, auraient toutefois pu être illégalement consultés.

Historique, cet incident n'est pourtant pas un phénomène isolé. Selon IBM Security[1], 8,5 milliards de données ont été compromises en 2019. Un chiffre en hausse de 200 %... en un an. Dans le domaine industriel, les attaques ont même bondi de 2 000 %. Relativement touché, le secteur de la santé figurait à la dixième du classement, toujours dominé par la finance. Les experts s'attendent néanmoins à une forte dégradation à court terme, en raison du contexte pandémique. « La cybersécurité doit devenir une priorité stratégique dans l'industrie pharmaceutique, commente David Gruson, directeur des programmes santé chez Jouve. Plutôt récente, la prise de conscience doit désormais s'accompagner d'une véritable politique de prévention et de gestion du risque. Ce sera l'un des principaux axes de structuration de la transformation numérique. »

Des risques accrus

Depuis un an, les fabricants de vaccins et les laboratoires de recherche sont dans le collimateur des hackers. Selon F-Secure[2], les cyberattaques contre les industries de santé ont augmenté de 14 %. Elles proviendraient principalement de Russie et de Chine. « La période actuelle est propice à la dématérialisation des échanges. Le contenu de certaines discussions ou le transfert de certains dossiers ont accentué

Fareva : un exemple caractéristique

Mercredi 16 décembre 2020. Deux heures du matin. Implanté en Seine-et-Marne, le data center de Savigny-le-Temple est infecté par un ransomware. Dix minutes plus tard, le système central est coupé par les informaticiens de permanence. Toutes les usines du groupe se retrouvent brusquement à l'arrêt ou presque. Deux d'entre elles continuent à fonctionner normalement, celles de Pau et de Vitré*. Choisi pour fabriquer le futur vaccin anti-Covid de l'allemand CureVac, le façonnier français accuse le coup. La "panne" aura finalement duré près d'un mois. Le montant des dégâts n'a pas encore été chiffré. Outre la perte d'activité, la plupart des 12 000 salariés ont été placés en chômage partiel. Aucune demande de rançon n'a jamais été formulée…

(*) Non connectées au système central, elles ont été épargnées.

la menace de manière quasi inédite », souligne Vincent Trely, président de l'APSSIS. Signe particulier, les laboratoires sont confrontés aux trois grands facteurs de risque : la cybercriminalité, le cyberespionnage et le cyberactivisme. « C'est ce qui les rend si singuliers dans le paysage des affaires ! »
Conjoncturelles, les causes sont aussi structurelles. La recrudescence des cas est corrélée à la digitalisation des pratiques sectorielles, symbolisée par l'essor de l'industrie 4.0. « La révolution technologique accroît considérablement la surface d'exposition », confirme-t-il. Outre les éléments scientifiques, cliniques ou pharmaco-épidémiologiques, la propriété intellectuelle, les projets de fusion ou d'acquisition, les plans de restructuration, les bilans chiffrés, les détails d'une négociation de prix ou encore les montants d'un appel d'offres hospitalier sont des informations hautement sensibles. « Les secrets industriels sont très prisés. Ils ont une valeur marchande et concurrentielle inestimable. Ils se revendent d'ailleurs à prix d'or sur des marchés parallèles », explique Jean-Jacques Zambrowski, économiste de la santé.

Des enjeux multiples

Dans son dernier rapport annuel[3], IBM Security évalue le coût total moyen d'une violation de données à 3,86 millions de dollars, tous secteurs confondus. A noter : la santé affiche la plus forte progression, soit 10,5 %. La facture s'élève à 7,13 millions. La taille des entreprises est également un critère différenciant. Pour un groupe pharmaceutique de plus de 25 000 salariés, la perte sèche atteint 5,52 millions de dollars. En dessous de 500 employés, elle tombe à 2,64 millions. Autre répercussion notable : le "temps d'arrêt" est estimé à 329 jours, contre 280 jours en moyenne. « La maturité des organisations est un paramètre déterminant. Les laboratoires dotés d'un plan de réponse aux incidents peuvent drastiquement réduire les délais et les impacts financiers », rappelle Vincent Trely.
Au regard des conséquences potentielles, les industriels n'ont pas vraiment d'autre alternative. Ils doivent impérativement s'emparer du sujet. « Ils doivent investir massivement dans les équipements techniques et les ressources humaines », préconise Jean-Jacques Zambrowski. Deux options sont envisageables : internaliser ces fonctions ou s'adosser à des opérateurs spécialisés. Le choix est ouvert, mais… « La maîtrise de l'infrastructure numérique doit être privilégiée. C'est une question de qualité, de souveraineté et de responsabilité. La politique de sécurité des systèmes d'information doit aussi s'appliquer aux co-traitants et aux sous-traitants », recommande David Gruson. Les experts en conviennent : le piratage de certains dispositifs médicaux connectés, à l'image des pompes à insuline ou des pacemakers, ne relève plus de la science-fiction. La pollution des chaînes de production industrielles non plus. Le cyberterrorisme n'est plus un simple fantasme. ■

Jonathan Icart

(1) « X-Force Threat Intelligence Index 2020 », IBM Security (février 2020).
(2) « Attack Landscape H1 2020 », F-Secure (septembre 2020).
(3) « Cost of Data Breach Report 20200 », IBM Security/Ponemon Institute (juillet 2020).


DR

Trois questions à... Laurent Heslault, président de Cyber-Résilience Consulting

Quel est le mode opératoire des cybercriminels ?

● Ces derniers temps, les pirates informatiques procèdent le plus souvent par le biais d'un ransomware. Ils réclament de fortes sommes d'argent pour restaurer des fichiers cryptés par un logiciel malveillant. De la même manière, ils peuvent subtiliser des données sensibles pour les revendre aux plus offrants. Ils agissent généralement par intérêt ou par idéologie politique. Ils peuvent notamment se livrer à des opérations de sabotage ou divulguer des informations confidentielles, sans rien attendre en retour. Dans tous les cas, ils utilisent des méthodes sophistiquées. Ils ont également recours à des modes de paiement intraçables. Ils sont donc très difficiles à débusquer. La réponse doit être mieux coordonnée à l'échelon international.

Quels sont les risques encourus par les laboratoires pharmaceutiques ?

● La cybersécurité soulève des enjeux techniques, humains, organisationnels et financiers. Pour un laboratoire, les coûts directs et indirects d'un vol de données se chiffrent en millions d'euros. Les liens d'interdépendance avec ses partenaires sont une zone de fragilité largement exploitée par les attaquants. En cas de fuite de données à caractère personnel, l'industriel sera tenu pour responsable, comme le prévoient les règlementations en vigueur. La révolution technologique accroît le niveau danger. La crise sanitaire aussi. Le phénomène prend incontestablement de l'ampleur. Au fil des années, le cyber-risque est progressivement devenu la principale menace pour les entreprises du monde entier. Le secteur pharmaceutique ne déroge pas à la règle, bien au contraire.

Quelles sont vos recommandations ?

● La dynamique doit être impulsée par les fonctions de direction. Elles doivent investir efficacement dans les infrastructures et les compétences. Elles doivent également sensibiliser et former leurs équipes. La souscription d'une cyberassurance n'est plus un luxe. Bien plus élevés, les impacts financiers d'un incident méritent d'y réfléchir. Face à un risque scélérat, il vaut mieux agir plutôt que subir. Autre recommandation majeure : les problématiques de sécurité informatique et de confidentialité des données doivent être davantage pensées en amont des projets. En cas d'attaque, la perte d'informations est parfois inévitable, mais il est possible de circonscrire les dégâts avec des mesures simples. Des solutions de stockage sécurisées doivent être privilégiées, à l'image des NAS. A tout le moins, le chiffrement des données sensibles est fortement recommandé.

Propos recueillis par Jonathan Icart