Deloitte.

SECTEUR SANTÉ ET SCIENCES DE LA VIE
FÉVRIER 2023

Uniquement une question de temps: la gestion des attaques par ransomware dans le secteur de la santé

Sommaire

Ces dernières années, le secteur de la santé à l'échelle mondiale a enregistré une hausse frappante des attaques par ransomware.

En 2022, les établissements de santé aux États-Unis ont fait l'objet de 1'410 cyberattaques par semaine en moyenne, ce qui constitue une hausse de 86% par rapport à 2021.[1] Simultanément, au Canada, les attaques par ransomware visaient pour la moitié d'entre-elles des entreprises de secteurs stratégiques, tels que la santé.[2] De même, les cyberattaques contre les réseaux hospitaliers et de santé en Europe ont augmenté de 47%[3] en 2020.

L'économie de la cybercriminalité est un facteur déterminant de cette augmentation. Cette activité lucrative génère plus de USD 1,5 billion par an.

Le bénéfice enregistré est incroyablement élevé, vu le coût moyen d'accès à une cible potentielle compris environ entre USD 400 et USD 0,0004.[4]

Quasiment une attaque par ransomware sur deux entraîne une violation de données,[5] faisant ainsi des deux incitations suivantes les choix de prédilection des cybercriminels : la vente de données personnelles rapportant environ USD 160 milliards par an et les rançons obtenues par ransomware environ USD 1 milliard par an.[6]

Voici deux domaines constituant le talon d'Achille du secteur de la santé: les réseaux hospitaliers et de santé.

Ils sont remplis de précieuses données, allant de données personnelles identifiables (PII) sensibles, d'informations sur les ordonnances et l'assurance maladie, aux dossiers internes des employés, dossiers financiers et la propriété intellectuelle. Une longue durée de conservation de la plupart de ces données facilite la vente de ces dernières et incite à d'autres crimes, tels que l'usurpation d'identité, l'extorsion ou la fraude.

Pour compliquer le tout, la récente pandémie a fourni de nouvelles possibilités d'attaque aux cybercriminels. Le passage rapide de l'industrie à un environnement virtuel a dévoilé de sévères lacunes au niveau des contrôles de cybersécurité, notamment en ce qui concerne les précieuses informations stockées au sein d'environnements informatiques complexes comportant souvent d'anciens systèmes et plates-formes personnalisés n'ayant pas été conçus pour un tel degré d'interconnexion.

À cela viennent s'ajouter des équipes de sécurité en sous-effectif et des cyberbudgets serrés. La raison pour laquelle le secteur de la santé est devenu la cible des cybercriminels va alors de soi.

Cela signifie malheureusement qu'une violation est presque inévitable. Vous avez malgré tout la possibilité de rendre votre entreprise moins intéressante pour les cybercriminels et de limiter les dommages en cas d'attaque. L'important est de répondre aux cybermenaces sophistiquées actuelles par une cyberdéfense efficace et de faciliter une reprise en toute confiance à l'issue d'une attaque.

Dans le présent article, nous explorons les différentes manières d'y arriver, afin que les organisations puissent tenir le rythme dans un paysage de cybersécurité évoluant rapidement.

Élaboration d'une stratégie de défense

La plupart des organisations admettent que les cyberadversaires ne sont plus des pirates isolés, mais des groupes de cybercriminels parfaitement organisés, des acteurs parrainés par des États et des réseaux du crime sophistiqués.

Bien que leurs attaques revêtent des formes différentes et proviennent de divers endroits, l'objectif visé reste toujours le même: causer le plus de dommages possibles à la cible pour que les organisations atteintes soient prêtes à payer la rançon.

Disposant de moyens financiers et de ressources, ces groupes arrivent à leurs fins de différentes façons. L'un des modèles d'attaque les plus courants dans le secteur de la santé est de faire appel à des initiés pour accéder de l'intérieur aux réseaux de l'organisation, en recrutant contre paiement des employés ou des entreprises contractantes agissant en interne pour ces groupes.

D'autres modèles infiltrent les systèmes de l'organisation par des attaques tierces visant notamment des applications web de base.[7]

Indépendamment de la manière dont les cybercriminels accèdent au réseau de l'organisation de santé, dans 93% des cas,[8] à l'issue de l'intrusion, l'accès à des ressources du réseau local n'est plus qu'un jeu d'enfant.

À partir de là, ils peuvent éteindre des systèmes stratégiques, bloquer l'accès à des informations et des données essentielles ou même pirater des dispositifs médicaux vitaux ou de maintien en vie connectés et exiger une rançon pour les débloquer.

En complément d'une violation des données à caractère personnel, ces attaques peuvent avoir d'autres conséquences dévastatrices, entraînant d'éventuels séjours à l'hôpital prolongés, des retards dans les procédures et les tests et même la mort de patients.[9]

Pour dissuader les intrusions, les organisations de santé devraient s'efforcer d'améliorer leur cyberdéfense, afin que les attaques soient plus complexes et coûteuses pour les acteurs malveillants. Dans le cas idéal, cela implique de se concentrer sur cinq domaines clés : la dissuasion des intrusions (voir page 04).

Dissuasion des intrusions

Mieux sensibiliser les utilisateurs
Les utilisateurs constituent souvent la première ligne de défense d'une organisation. Une formation ciblée sur la cybercriminalité et une sensibilisation à cette dernière ainsi qu'une surveillance continue des performances des groupes d'utilisateurs permettent de mieux empêcher les intrusions de pirates.

Réduire la surface d'attaque
Les pirates préfèrent attaquer les organisations là où elles sont le plus vulnérables. Il devient donc crucial de réduire votre surface d'attaque, grâce à la gestion active des vulnérabilités, à des systèmes à jour et renforcés ainsi qu'à la sécurité des utilisateurs finaux (l'isolement du navigateur p. ex.).

Améliorer le taux de détection
Avec un cyberpaysage en constante évolution, il convient de surveiller en permanence votre environnement afin de détecter tout comportement inhabituel ou signe d'attaque, tel que des activités suspectes de fichiers sur des périphériques de stockage.

Limiter les mouvements latéraux
Si un pirate parvient à accéder à vos systèmes, vous tentez d'empêcher toute propagation du dommage potentiel.

L'application des principes de la Confiance Zéro, tels que la gestion des identités et des accès privilégiés ainsi que la segmentation réseau, vous permet de restreindre la capacité des attaquants à se déplacer latéralement dans le réseau.

Isoler et maîtriser
Plus vous isolerez rapidement les systèmes affectés, mieux vous pourrez maîtriser les dommages consécutifs. L'un des moyens de faciliter cette tâche consiste à intégrer proactivement des fonctions de cloisonnement au concept d'infrastructure.

"Pour dissuader les intrusions, les organisations de santé devraient s'efforcer d'améliorer leur cyberdéfense, afin que les attaques soient plus complexes et coûteuses pour les acteurs malveillants."

Résilience et maintien des opérations critiques

Bien qu'une stratégie de défense puissante constitue un élément clé de la cybersécurité, la capacité de votre organisation à réagir à une violation est également importante.

Des temps de réaction courts et une capacité à réagir immédiatement à une attaque par ransomware améliorent considérablement la résilience de l'organisation, réduisent le risque de chantage et peuvent même sauver des vies, dans les cas extrêmes.

Cela signifie mettre en œuvre des capacités de réponse et de reprise et préparer vos équipes d'intervention pour qu'elles sachent déjà quoi faire avant que l'incident ne se produise.

Mettre en œuvre des capacités de réponse et de reprise

Pour une organisation prête et bien adaptée
Afin que votre organisation fonctionne comme une machine bien rodée en cas d'incident, il est utile de mettre en place à l'avance des équipes pluridisciplinaires de crise et d'intervention et de faciliter la reprise à l'échelle de l'entreprise, à l'aide d'entraînements, d'exercices, de simulations de crise et d'analyses rétrospectives d'incidents.

Planifier la reprise
Des plans techniques et non <techniques ainsi que des scénarios permettent à votre organisation de parcourir une à une les étapes de la reprise et de déterminer les opérations à privilégier en fonction de leur importance stratégique. Une compréhension globale de toute la chaîne de valeur est indispensable pour déterminer les priorités et les séquences de reprise.

Avoir les outils de reprise à portée de la main
Pour rétablir une infrastructure atteinte, il faut disposer des bons outils et du matériel qui convient. Il peut s'agir de copies inaltérables de données, d'environnements de reprise individuels ainsi que de l'orchestration et de l'automatisation de la reprise, tous ces outils pouvant accélérer considérablement la procédure de reprise.

Gérer la capacité en rafale
Pour lutter efficacement contre une attaque en cours, vous devez pouvoir allouer des ressources là où elles sont insuffisantes et acheminer celles en surplus. Cela est valable pour tous les types de ressources, des ressources physiques aux services de tiers.

Communiquer efficacement
Lors d'une violation, votre organisation a besoin de voies de communication et de procédures claires ainsi que de la capacité de rester transparente tout au long de l'intervention et d'inciter sans cesse le personnel au calme et à la maîtrise. Un plan de communication à toute épreuve, répondant à la fois aux besoins de communication interne et externe, peut aider à coordonner la reprise de manière posée et ciblée.

Cela est particulièrement important pour les organisations de santé: vous risquez d'avoir besoin de communiquer avec les patients et les autorités suivant la nature sensible et la quantité de données atteintes.

Reprise en toute confiance

Les organisations de santé doivent s'adapter, au fur et à mesure que les cybermenaces évoluent.

Cela signifie aller au-delà de la détection des cyberattaques et de la protection des actifs critiques pour développer une reprise en souplesse en cas d'incident.

Dans certains cas, la réparation de systèmes endommagés et de grandes quantités de données corrompues peut s'avérer nécessaire.

Dans d'autres cas, cela peut nécessiter la mise en œuvre de plans pour éviter l'interruption d'exploitation en cas de pannes prolongées.

De toutes manières, les organisations de santé sont tenues de jeter les bases de la protection de leurs patients, en maintenant les systèmes essentiels en fonctionnement.

Cette tâche devient de plus en plus ardue, au fur et à mesure que les cybermenaces évoluent. Être prêt au préalable devient plus que jamais nécessaire.

En identifiant vos services stratégiques, en comprenant l'interaction entre vos différents systèmes, en entamant une formation continue et en perfectionnant sans cesse votre capacité à la reprise, vous contribuerez grandement à parer aux attaques, dont vous allez faire de plus en plus l'objet.

Pour communiquer avec nous

Notes de fin d'ouvrage

1 *https://www.securitymagazine.com/articles/98810-global-cyberattacks-increased-38-in-2022*

2 *https://globalnews.ca/news/8427930/canadian-health-energy-sectors-increasingly-targeted-by-ransomware-attacks/*

3 *https://www.balcanicaucaso.org/eng/Areas/Europe/Cyber-attacks-are-growing-in-the-European-Union-21652*

4 *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

5 *https://www.kroll.com/en/insights/publications/cyber/ransomware-attack-constitute-data-breach*

6 *https://www.techrepublic.com/article/cybercriminals-raking-in-1-5-trillion-every-year/*

7 *https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf*

8 *https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=70ea31106b61*

9 *https://www.ibm.com/thought-leadership/institute-business-value/report/medical-device-security*

Kishwar Chishty
Partner – Global LSHC Industry Cyber Leader – Deloitte Switzerland
Life Sciences Risk Advisory

kchishty@deloitte.ch

Florian Widmer
Partner – Deloitte Switzerland
Cyber and Strategic Risk

fwwidmer@deloitte.ch

John Lu
Principal – Deloitte & Touche LLP
Cyber and Strategic Risk

jolu@deloitte.com

Deloitte.