rubrik

Pourquoi vous pensez être bien préparé à une cyberattaque, alors qu'il n'en est rien !

- **Vous avez installé Rubrik, mais votre entreprise vous laissera-t-elle l'utiliser pendant une cyberattaque ?**
- **Quels sont les facteurs susceptibles de vous ralentir dans votre capacité de restauration, hormis vos plateformes de cyber-résilience ?**
- **Vous avez peut-être déjà mis en place un plan de cyber-restauration, mais avez-vous pensé à y inclure des autorisations de communication spécifiques ?**

Au cours d'une cyberattaque, tout le monde est sur le pont. Bon nombre d'organisations ont déjà pris des mesures pour se préparer à de tels scénarios. Mais l'expérience montre que ces plans présentent souvent des failles, et pour cause : soit ils sont élaborés en anticipant d'autres scénarios qu'une cyberattaque, soit ils représentent des scénarios qui ne reflètent pas des menaces qui sont actuellement recensées dans le monde réel. Il n'est pas très judicieux (et surtout il est extrêmement coûteux) d'attendre qu'une attaque se produise pour repérer ces failles. Une bonne préparation à ce type de situation peut faire toute la différence : elle peut vous aider à restaurer vos charges de travail en seulement quelques minutes, sans risque d'y passer plusieurs heures, jours ou semaines, voire d'essuyer tout simplement un échec. Songez au temps d'indisponibilité que votre entreprise serait capable de tolérer. Certains services métiers ou certaines capacités techniques ont-ils une importance tout particulièrement stratégique pour votre organisation ? Toutes les parties prenantes s'accordent-elles sur ce point ?

Toutes les entreprises sont différentes, certes, mais nous allons ici tâcher de mettre en évidence certaines failles identifiées dans les plans de reprise de nombreux clients victimes de cyberincidents pour lesquels est intervenue l'équipe de réponse aux ransomwares de Rubrik. Pour obtenir d'autres recommandations qui vous guideront dans l'élaboration de vos plans de réponse aux incidents, Rubrik met à votre disposition un cadre complet présenté sous la forme d'un livre blanc, téléchargeable ici. Rubrik Security Cloud propose plusieurs fonctionnalités conçues pour vous aider à réduire votre surface d'attaque potentielle, à détecter les cyberattaques et à réagir en conséquence. Ce document comprend un ensemble de pratiques que les clients de Rubrik peuvent mettre en œuvre pour avoir la certitude que l'ensemble de leurs parties prenantes métiers et techniques connaissent les outils dont elles disposent. Ces bonnes pratiques sont particulièrement utiles dans le cadre de l'élaboration des plans de reprise.

AMÉLIORER LE DEGRÉ DE PRÉPARATION

Anticipez ! Passez en revue vos plans de reprise avant d'être frappé par une cyberattaque. Cette vérification doit suivre un processus itératif et impliquer toutes les parties prenantes de vos équipes métiers et technologiques. L'idéal est de répéter ce processus chaque trimestre, pour être certain que vos plans sont à jour et qu'ils reflètent tous les scénarios qui inquiètent vos parties prenantes. Envisagez une grande diversité de scénarios : la violation d'une seule pile applicative ou d'un service métier donné, ou même la perte totale de vos systèmes de production et de tous les canaux de communication officiels (e-mails, messagerie instantanée, systèmes téléphoniques d'entreprise, etc.). Il est probable que ce processus soulève de nombreuses interrogations chez les parties prenantes. Il est important d'engager ces discussions avant une attaque, car dès lors que vous passez en mode intervention d'urgence, chaque seconde compte. Par exemple, si, au cours d'un incident, vous vous rendez compte que vous devez négocier des accords de confidentialité, il sera certainement bien plus difficile de restaurer rapidement votre environnement ; de nombreuses organisations en ont d'ailleurs fait les frais.

N'oubliez pas non plus qu'il vous faudra probablement plusieurs plans pour gérer différents scénarios. Par exemple, il est indispensable d'élaborer un plan de reprise après sinistre, mais ce type de plan ne sera pas nécessairement utile face à un cyberincident. Vous pourrez certainement réutiliser de nombreux éléments de votre plan de reprise après sinistre pour répondre à un incident (par exemple, procédure de restauration des piles applicatives, identification des services stratégiques, etc.), mais il n'en reste pas moins important d'en évaluer les différences.

QUESTIONS À POSER OU ÉLÉMENTS À COMMUNIQUER AUX PARTIES PRENANTES MAINTENANT QUE VOUS BÉNÉFICIEZ DE LA PROTECTION RUBRIK :

Votre équipe de sécurité sait-elle que vos données sont protégées par Rubrik ?

Pourquoi est-ce important ?
Les capacités de sécurité et de réponse offertes par Rubrik couvrent une grande diversité de domaines : protection des données, enquête sur incident, recherche de menaces, découverte de données sensibles, détection de l'onde de choc, enquête criminelle, isolement des menaces, mesures correctives et restauration des données. L'équipe de sécurité doit impérativement connaître ces différentes fonctionnalités et être en mesure de les utiliser en cas d'attaque afin d'en atténuer les répercussions sur votre organisation.

Vos applications et systèmes critiques sont-ils sauvegardés/protégés par Rubrik ?

Pourquoi est-ce important ?
Quand les systèmes critiques sont à l'arrêt, tout devient une course contre la montre. L'équipe opérationnelle et l'équipe de réponse aux incidents doivent savoir si elles disposent d'une copie saine des systèmes et données ciblés par l'attaque afin de pouvoir l'exploiter pour restaurer l'environnement.

À qui devez-vous poser cette question ?
À votre équipe des opérations IT

Votre équipe a-t-elle signé un accord de confidentialité avec Rubrik ?

Pourquoi est-ce important ?
Votre équipe juridique peut vouloir mettre en place un accord de confidentialité supplémentaire en cas de cyberincident. Si c'est le cas, veillez à ce que cet accord ait été négocié et que les termes aient été convenus en amont, de manière à pouvoir communiquer rapidement et en toute transparence avec l'équipe de réponse aux ransomwares de Rubrik, et ainsi gagner un temps précieux au moment de la restauration.

À qui devez-vous poser cette question ?
À votre équipe juridique et à votre responsable de compte Rubrik

Faites en sorte que votre équipe juridique, votre direction et votre responsable de la continuité d'activité sachent que vous avez signé un accord de confidentialité avec Rubrik.

Pourquoi est-ce important ?
Il est important que toutes ces parties prenantes comprennent que Rubrik est un partenaire de confiance qui soutiendra l'entreprise dans ses efforts de restauration. Rubrik respecte scrupuleusement la confidentialité de chaque interaction client et s'engage à ne divulguer aucune information à un tiers. Le fait d'intégrer Rubrik peut contribuer à accélérer le déroulement des activités de découverte, de confinement et de correction, tout en évitant les retards coûteux et en permettant à vos équipes d'évaluer les impacts et de formuler des plans de reprise.

À qui devez-vous poser cette question ?
À votre responsable juridique, à votre direction et à votre responsable de la continuité d'activité

Votre cyberassurance impose-t-elle des limites quant à l'identité des intervenants avec lesquels votre équipe de réponse est autorisée à collaborer au cours d'un cyberincident ?

Pourquoi est-ce important ?
Quiconque prend part à la résolution d'un incident aspire toujours à produire le meilleur résultat pour l'organisation victime. Il n'est pas rare de vouloir limiter la connaissance des faits et la circulation des informations au-delà des murs de l'organisation compte tenu des actions potentielles.

À qui devez-vous poser cette question ?
À votre compagnie d'assurance

Que faut-il faire ?
Il est important d'informer au préalable tous ceux qui participent aux efforts de réponse et de résolution, y compris votre compagnie d'assurance, du rôle essentiel que jouera l'équipe de réponse aux ransomwares de Rubrik pour comprendre l'onde de choc et les options de récupération au cours d'un incident. Cette précaution permettra de réagir plus rapidement et de réduire le délai moyen de restauration.

Faites-vous appel à un prestataire externe de réponse aux incidents ?

Pourquoi est-ce important ?
Notre propre équipe de réponse aux ransomwares est souvent amenée à collaborer avec des équipes de réponse aux incidents tierces, qui interviennent sur le site du client pour comprendre l'onde de choc d'un incident et initier les activités de recherche de menaces, afin de restaurer le plus rapidement possible les données et les services métiers. Pour accélérer le travail d'évaluation et de récupération, il est essentiel également d'informer ces tiers en amont que votre entreprise fait confiance à l'équipe de réponse aux ransomware de Rubrik.

À qui devez-vous poser cette question ?
À vos équipes responsables de la sécurité de l'information, de la résilience/continuité d'activité, du pôle juridique et des achats.

Avez-vous identifié, documentation à l'appui, des systèmes métiers ou des services métiers à restaurer en priorité ?

Pourquoi est-ce important en cas d'incident ?
Les parties prenantes chercheront à savoir si des systèmes stratégiques sont touchés et, le cas échéant, sous quel délai ils seront à nouveau disponibles. Il est important de s'entendre sur ces questions au préalable, de manière à réduire l'incertitude, à prioriser les efforts de restauration et à communiquer efficacement avec les personnes concernées.

Pourquoi est-ce important pour la récupération ?
Au cours d'un incident, il est essentiel de réduire autant que possible le délai de reprise. Le fait de définir clairement un ensemble de priorités contribue à simplifier grandement la collaboration entre les différentes équipes (opérationnelles, métiers, techniques, sécurité, continuité), tout en accélérant les efforts de restauration.

À qui devez-vous poser cette question ?
Aux équipes responsables de la continuité d'activité intervenant dans les directions technologiques et dans certaines directions métiers, qui auront très certainement identifié ces priorités.

RÉSUMÉ

Face au manque de temps, même quand tout se passe bien, il peut être assez difficile de fédérer l'ensemble des parties prenantes autour de l'élaboration de plans et de procédures d'action en cas de cyberattaque. Malheureusement, c'est précisément sur ce scénario que misent les cybercriminels, qui ne cessent de faire des ravages. C'est pourquoi il est vital de bien se préparer. Suivez les recommandations de ce document pour vous préparer, votre entreprise et vous-même, à déjouer sereinement les attaques ennemies.