MENACES À LA CYBERSÉCURITÉ DANS LE SECTEUR MINIER CANADIEN : VOTRE ENTREPRISE Y EST-ELLE PRÉPARÉE?

Publié le 13 janvier, 2023

Catégories: Perspectives, Publications

Les cyberattaques visant les infrastructures essentielles sont en hausse, et présentent d'importantes conséquences potentielles pour les économies nationales et mondiale. Parmi les menaces les plus connues auxquelles sont exposées les organisations figurent les rançongiciels, des logiciels malveillants qui menacent de publier les données de la victime ou de bloquer l'accès à un système à moins qu'une rançon ne soit payée. Les menaces par rançongiciel interrompent des fonctionnalités critiques dépendant d'une connexion réseau ou système, ce qui peut entraîner des conséquences dévastatrices. Au premier semestre de 2021, elles ont connu une hausse effarante de 151 % à l'échelle du globe.

Au Canada, le secteur minier est depuis longtemps un maillon essentiel des infrastructures critiques, en raison de sa production de matériaux bruts servant à la fabrication d'équipement et de biens nécessaires. C'est pourquoi les entreprises de ce secteur sont particulièrement vulnérables aux cyberattaques. Elles sont une cible de choix pour plusieurs raisons : leur grande dépendance à la technologie, leur besoin de communication constante et fiable en région isolée, et le fait que les minéraux extraits ont en soi une grande valeur, en plus d'être essentiels à la production d'importantes technologies partout dans le monde. Plusieurs attaques notables sont survenues récemment, dont celles largement publicisées à l'endroit de Nvidia, de Kaseya et de Colonial Pipeline. Le 27 décembre 2022, l'attaque par rançongiciel contre Copper Mountain Mining a entraîné la fermeture de sa mine du sud-ouest de la Colombie-Britannique pendant près d'une semaine, ainsi qu'une chute immédiate de 5,5 % du cours de l'action.

Conséquences des cyberattaques

Les attaques par rançongiciel entraînent souvent l'interruption complète des activités; c'est sans doute l'une des formes de cybercriminalité les plus nuisibles à une société minière. L'interruption des systèmes d'exploitation, de sécurité et de traitement représente de lourds dommages financiers pour les sociétés minières, sans compter les effets sur les données sensibles, dont les renseignements personnels (endommagement, destruction ou communication). Les conséquences des cyberattaques par rançongiciel sont graves. Certaines sont immédiates, d'autres sont durables : perte de confiance, mauvaise réputation aux yeux du public, risques pour l'image et investisseurs inquiets.

À grande échelle, les incidents de sécurité comme les attaques par rançongiciel causent de graves difficultés financières, réglementaires et opérationnelles pour une société :

1. compromission d'actifs informationnels clés (renseignements confidentiels et personnels, secrets commerciaux, propriété intellectuelle d'importance);
2. interruption des activités, faute d'un accès aux systèmes d'information essentiels;
3. surveillance réglementaire accrue (plaintes, enquêtes, etc.);
4. risques de responsabilité civile;
5. extorsion par les pirates.

Les conséquences sont telles que bien des sociétés acceptent de payer les rançons demandées pour pouvoir reprendre leurs activités le plus vite possible. Cependant, cela n'atténue pas nécessairement les conséquences. Un récent sondage auprès d'entreprises canadiennes révélait que seules 42 % des organisations ayant payé une rançon avaient retrouvé la totalité de leurs données. Sachant cela, mieux vaut mettre en place des processus et des protections de cybersécurité robustes, ainsi que des programmes rigoureux de protection des renseignements personnels.

Intervention en cas d'incidents de cybersécurité

Les sociétés minières sont vivement encouragées à mettre en place des plans et des processus non seulement pour se protéger des cyberattaques, mais aussi pour savoir comment y répondre, le cas échéant. Il est impossible d'éliminer tout à fait les risques, mais on peut atténuer tant l'exposition de l'organisation à ces risques que leurs conséquences en préparant un plan d'intervention. Une société devrait au minimum :

1. déterminer qui sont les principaux membres de son équipe d'intervention, et comment et quand ils communiqueront en cas d'incident;
2. faire l'inventaire des données sensibles et exclusives contenues dans les systèmes de l'organisation ou dans ceux de tiers et des obligations légales découlant de leur compromission;
3. veiller à ce qu'il y ait en place des politiques et procédures critiques pour limiter l'exposition au risque en cas d'incident (comme une politique adéquate de rétention et de destruction de documents);
4. envisager de souscrire une assurance contre les cyberrisques.

Le plan d'intervention en cas de cyberattaque doit protéger votre organisation dans l'immédiat, mais aussi à long terme. Son contenu dépendra des caractéristiques et des besoins de la société. Le plan peut avoir différentes visées :

1. planification de services d'intervention efficaces en cas d'incident, par exemple, attaques par rançongiciel, espionnage interne, erreurs d'envoi de courriels;

2. recommandation et mise en œuvre d'une stratégie de reddition de comptes et d'avis aux fins de conformité aux obligations légales et de réduction de risques de litiges;
3. rédaction d'avis internes et publics et de foires aux questions pour atténuer les risques de litiges et pour la réputation.

Conclusion

Les attaques par rançongiciel évoluent et deviennent de plus en plus complexes grâce aux nouvelles technologies; elles demeureront une menace omniprésente pour toutes les entreprises, mais particulièrement celles du secteur minier. McMillan peut vous aider à mettre en place des stratégies de prévention et de lutte contre les incidents de cybersécurité, et vous aider à y réagir le cas échéant.

par Robert Piasentin, Mitch Koczerginski, Kristen Shaw et Gemma Walsh (stagiaire)

Mise en garde