La mine intelligente actuelle et future : le défi de la cybersécurité

Par Nicholas Théroux
Institut national des mines
Collaborateur

D'année en année, les études successives démontrent que la quantité de cyberattaques que subissent les entreprises ne cesse d'augmenter. Le Forum économique mondial (FEM, 2019) estime d'ailleurs qu'à l'échelle mondiale le montant des pertes financières liées à la cybercriminalité a quadruplé entre, 2015 et 2019, pour s'établir à plus de 2,1 billions de dollars américains. La vague de cyberattaques ayant ciblé plusieurs compagnies minières canadiennes entre 2013 et 2016 et s'étant soldée par le vol d'une grande quantité de données corporatives a démontré que même les entreprises œuvrant dans le secteur minier n'y échappent pas (Jenish, 2019). L'enjeu de la cybersécurité est donc désormais à considérer dès l'implantation des nouvelles technologies, notamment celles menant vers la mine intelligente.

Source : Institut national des mines du Québec

La protection des données, un défi croissant

En 2018, une enquête menée par Scalar Decisions (2018) auprès de 421 entreprises canadiennes a révélé que près de neuf sociétés canadiennes sur dix déclaraient avoir été victimes d'une cyberattaque réussie au cours de la dernière année. À l'ère de l'industrie 4.0, de plus en plus d'objets sont connectés à Internet, faisant en sorte que la surface d'attaque devient de plus en plus étendue. Les pirates profitent donc de cette multiplication des possibilités d'intrusion afin de perpétrer des cyberattaques toujours plus sophistiquées. D'ailleurs, ces cyberattaques ne menacent plus seulement les réseaux informatiques des organisations, mais également les technologies opérationnelles que celles-ci utilisent pour mener à bien leurs activités industrielles. En effet, la révolution industrielle 4.0 repose en partie sur le recours à l'Internet des Objets (IdO), c'est-à-dire l'intégration des systèmes informatique et opérationnel (Ewing, 2018). Bien que cette connexion entre les deux systèmes permette d'optimiser la production, l'intégration entre les technologies de l'information (TI) et les technologies opérationnelles (TO) augmente l'ampleur des dégâts qu'un piratage peut causer. Ayant accès au réseau informatique, les pirates peuvent ainsi pousser plus loin leur intrusion et s'attaquer au système opérationnel qui permet, entre autres, de surveiller ou de contrôler les équipements servant à réaliser les diverses activités industrielles.

Par exemple, en 2014, une aciérie située en Allemagne a vu l'un de ses hauts fourneaux détruit par une hausse de température engendrée par un piratage. Après enquête, il a été déterminé que les pirates ont réussi à accéder au réseau informatique de l'aciérie grâce à une cyberattaque de type « harponnage »[1], puis à dérégler le haut fourneau en passant par un réseau opérationnel qui n'était pas séparé du réseau informatique (Howard, 2017). Dans le secteur minier, Deloitte (2018) men-

tionne que cette interconnexion entre les TI et les TO, caractérisant les nouvelles technologies issues de l'industrie 4.0, pourrait avoir des incidences particulièrement fâcheuses en cas de cyberattaque réussie ; par exemple, les pirates pourraient prendre le contrôle de systèmes de transport autonomes, endommager certains équipements et, donc, mettre la vie des travailleuses et des travailleurs en danger (Deloitte, 2018).

La cyberrésilience de la main-d'œuvre du secteur minier

Selon la firme Scalar Decisions (2018, p. 23), les employés sont l'« un des maillons les plus faibles de la sécurité des organisations ». Pour la firme Willis Towers Watson (2017), cette déclaration découle du constat que la majorité des brèches dans la cybersécurité des organisations sont le fruit de comportements numériques inadéquats de la part de travailleuses ou de travailleurs. D'ailleurs, Scalar Decisions (2018) identifie le manque de formation en sécurité informatique et en gestion de données confidentielles comme étant les facteurs majeurs expliquant pourquoi la main-d'œuvre constitue le maillon faible de la cybersécurité des entreprises.

Dans son rapport intitulé « *An integrated approach to combat cyber risk: securing industrial operations in mining* », la firme de conseil Deloitte (2018) soutient qu'à l'image des autres secteurs industriels, l'industrie minière doit porter une attention particulière à la protection de ses systèmes de contrôle industriel puisque l'intégration entre les TI et les TO rend possible des cyberattaques affectant les équipements connectés. Or, la main-d'œuvre minière ne serait pas toujours convenablement formée afin de pouvoir reconnaître rapidement les cyberattaques, notamment, parce que ces dernières prennent des formes de plus en plus sophistiquées. De plus, toujours selon Deloitte (2018), plusieurs travailleuses et travailleurs qui œuvrent sur le terrain avec des équipements connectés ne réalisent pas que les appareils qu'ils utilisent dans leurs tâches quotidiennes sont maintenant à risque d'être la cible d'une cyberattaque. Cette perception fait en sorte que certains membres du personnel ne respectent pas les protocoles de sécurité requis puisqu'ils considèrent que ceux-ci sont plus ou moins utiles. Bien qu'au cours des dernières années la plupart des entreprises du secteur minier aient mis en place des mesures rigoureuses afin d'augmenter leur niveau de protection face aux cybermenaces, il devient maintenant nécessaire d'étendre la formation et la sensibilisation en cybersécurité à tous les employées et les employés des organisations. Par ailleurs, même les membres du personnel travaillant sur le terrain peuvent désormais être confrontés aux conséquences directes ou indirectes d'une cyberattaque.

Comment préparer les travailleuses et les travailleurs du secteur minier à faire face à cet enjeu ?

Une entreprise du secteur minier qui souhaite augmenter sa cybersécurité grâce à l'amélioration de la cyberrésilience de son personnel peut poser plusieurs actions. Selon l'étude « *From technology to people: The new frontier in mining cyber risk Mining Risk Review 2017* » de Willis Towers Watson (2017), il est recommandé de procéder, notamment grâce à l'implication du département informatique de l'entreprise, à un recensement des compétences en cybersécurité qui font défaut au sein de l'organisation. Une fois que les compétences insuffisamment maîtrisées sont connues, l'entreprise peut alors mettre en place une stratégie de formation ciblant l'acquisition de celles-ci dans les plus brefs délais. De plus, des tests de préparation aux cyberattaques peuvent être réalisés de façon régulière. Ces tests consistent à lancer de fausses cyberattaques afin d'évaluer la manière dont réagissent les membres du personnel en plus de mesurer leur niveau de vigilance. Selon Deloitte (2018), de tels tests permettent notamment d'évaluer si les pro-

L'IRME, un institut de recherche reconnu internationalement pour ses expertises uniques!

- Caractérisation minérale et prédiction géochimique
- Gestion et valorisation des rejets
- Traitement des eaux minières
- Remblais souterrains et géotechnique minière
- Restauration des sites miniers et plus encore!

uqat.ca/irme

UQAT

Source : Institut national des mines du Québec

cédures de sécurité sont respectées, puis de procéder aux formations complémentaires qui sont jugées nécessaires et ce, en fonction des résultats obtenus.

En conclusion, la formation des travailleuses et des travailleurs constitue l'un des meilleurs retours sur investissement qu'une entreprise puisse réaliser lorsqu'elle décide de consacrer des ressources financières à l'amélioration de sa cybersécurité. Pour cette raison, l'acquisition de savoir-faire en cybersécurité chez la main-d'œuvre du secteur minier doit être considérée, selon Morgan (2018), comme un investissement plutôt qu'une dépense. Après l'organisation d'un premier colloque portant notamment sur ce sujet en novembre dernier, l'Institut national des mines publiera au cours de l'année 2020 une étude portant notamment sur le savoir-faire en cybersécurité dans des programmes de formation menant au secteur minier québécois et ce, dans les trois ordres d'enseignement. **RMI**

Note

[1] Selon l'Office québécois de la langue français (2019), l'harponnage est une « Technique d'hameçonnage qui, à l'aide de courriels trompeurs et personnalisés, cible de façon plus précise un groupe d'internautes donné, souvent les employés d'une grande société ou d'un organisme gouvernemental, afin de leur soutirer des renseignements confidentiels permettant ensuite de pénétrer les systèmes informatiques.

Références

(1) Deloitte. (2018). An integrated approach to combat cyber risk: securing industrial operations in mining. Récupéré le 17 octobre 2019 de : https://www2.deloitte.com/global/en/pages/energy-and-resources/articles/approach-to-combat-cyber-risk-mining.html

(2) Ewing, Ian. (2018). Mine security in the digital age : with more mines being connected, how are they being protected? CIM Magazine. Récupéré le 21 octobre 2019 de : https://magazine.cim.org/en/technology/mine-security-in-the-digital-age-en/

(3) Forum économique mondial. (2019). Here's how we can tackle the growing cybersecurity skills gap. Récupéré le 17 octobre 2019 de : https://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurity-skills-gap/

(4) Howard, Solomon. (2017). Canadian cyber attack lead to new mining industry threat sharing center. IT World Canada. Récupéré le 17 octobre 2019 de : https://www.itworldcanada.com/article/canadian-cyber-attack-led-to-new-mining-industry-threat-sharing-centre/393850

(5) Jenish, D'Arcy. (2018). Miners band together to fight cyber-criminals: how the industry is fighting back and beefing up cyber-security. Canadian Mining Journal. Récupéré le 17 octobre 2019 de : http://www.canadianminingjournal.com/features/miners-band-together-to-fight-cyber-criminals/

(6) Morgan, Steve. (2018). Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. Cybercrime Magazine. Récupéré le 25 octobre 2019 de : https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

(7) Office de la langue française (2019). Fiche terminologique « harponnage ». En ligne. URL : http://www.granddictionnaire.com/ficheOqlf.aspx?Id_Fiche=8349460, Consulté le 11 novembre 2019.

(8) Scalar Decisions. (2018). État de préparation en matière de cybersécurité des organisations canadiennes : résultats de l'étude sur la sécurité 2018 de Scalar. Toronto : Scalar Decisions. Récupéré le 17 octobre 2019 de : https://www.scalar.ca/fr/landing/etude-securite-2018-de-scalar/

(9) Willis Towers Watson. (2017). From technology to people: The new frontier in mining cyber risk Mining Risk Review 2017. Londres : Willis Towers Watson.