MARSH

Mining in 10 – Cyber – Transcript

French Canadian Translation

4
00:00:11.380 --> 00:00:22.419
Raul Munoz : Bienvenue de retour à Mines en 10 minutes. Je suis Raul Munoz chez Marsh, et dans l'épisode d'aujourd'hui, nous nous penchons sur l'une des catégories de risque qui connaît la plus forte croissance dans notre industrie, votre risque cyber.

5
00:00:22.570 --> 00:00:39.739
Raul Munoz : Comme nous le savons tous, l'exploitation minière a connu une transformation numérique remarquable au cours des dernières années. Des camions autonomes à la surveillance à distance en passant par les capteurs IoT, l'analyse en temps réel, toute cette technologie a rendu les opérations plus sûres et beaucoup plus efficaces.

6
00:00:39.920 --> 00:00:56.360
Raul Munoz : Mais cela a aussi ouvert les portes à ce qui n'existait pas avant, le risque cyber. Mon invité d'aujourd'hui est Julien Ducloy, qui est un spécialiste du risque cyber chez Marsh Risk et travaille spécifiquement avec des clients industriels et miniers. Alors, commençons. Merci beaucoup de m'avoir rejoint, Julien.

7
00:00:57.380 --> 00:00:58.919
Julien Ducloy : Merci, Raul. Je suis heureux d'être ici.

8
00:01:00.000 --> 00:01:05.750
Raul Munoz : Commençons par les bases. Quels types de risque cyber les chefs de file du secteur minier devraient-ils envisager ?

9
00:01:06.880 --> 00:01:09.920
Julien Ducloy : Donc, à un haut niveau, il y a deux catégories.

10
00:01:10.030 --> 00:01:28.580
Julien Ducloy : Les attaques ciblées, où un cybercriminel s'en prend délibérément à une organisation spécifique, généralement parce qu'il connaît un actif particulier, il veut accéder à des données précieuses, ou il cherche à causer des perturbations pour des raisons concurrentielles ou géopolitiques.

11
00:01:28.920 --> 00:01:42.830
Julien Ducloy : Et l'autre catégorie est les attaques non ciblées ou les attaques à large diffusion, où l'attaquant lance essentiellement un large filet. Les logiciels de rançon déployés largement, les campagnes de phishing, pour obtenir l'accès aux identifiants.

12
00:01:42.830 --> 00:01:49.589
Julien Ducloy : Ou des vulnérabilités analysées sur le web, et ils espèrent attraper quiconque n'est pas adéquatement protégé.

13
00:01:50.580 --> 00:02:07.299
Raul Munoz : C'est intéressant, parce que généralement, quand... quand on pense aux cyberattaques, nous... l'exploitation minière n'est pas nécessairement... n'est pas la première chose qui vient à l'esprit. Alors, quel genre de conséquences une cyberattaque réussie pourrait-elle avoir pour... spécifiquement pour les entreprises minières ?

14
00:02:07.900 --> 00:02:27.619
Julien Ducloy : Elles peuvent être graves et il y a une large gamme de conséquences. Nous avons vu de nombreux incidents dans le passé, différents types d'incidents dans l'industrie minière, et à l'extrémité la plus grave, vous parlez d'attaques contre la technologie opérationnelle, c'est-à-dire les systèmes qui contrôlent l'équipement physique.

15
00:02:27.650 --> 00:02:36.550
Julien Ducloy : Et si un attaquant obtient l'accès à un système de contrôle minier, il pourrait manipuler le comportement de l'équipement, créer des risques pour la sécurité et perturber la production.

16
00:02:36.770 --> 00:02:51.320
Julien Ducloy : En même temps, l'attaque contre les systèmes informatiques peut entraîner le vol de données d'exploration, d'informations financières, de métriques de production également, et ces informations ont une valeur concurrentielle énorme.

17
00:02:51.330 --> 00:03:07.199
Julien Ducloy : Et enfin, je veux dire, nous en avons tous entendu parler, les attaques par rançongiciel, qui ciblent les systèmes IT et OT, maximisent réellement l'effet de levier et peuvent être assez dévastateurs.

18
00:03:07.900 --> 00:03:21.569
Raul Munoz : Ouais, vous savez, c'est intéressant, parce que quand on pense au parcours et au cycle de vie d'une entreprise minière, il y a évidemment différents niveaux de l'exploration jusqu'à la restauration, et je pense que l'un des plus

19
00:03:21.570 --> 00:03:30.589
Raul Munoz : chapitres intéressants du Guide de résilience sont les cadres décrits au chapitre 3.

20
00:03:30.590 --> 00:03:48.299
Raul Munoz : Où, vous savez, nous parlons de ces différentes expositions tout au long des différents cycles. Pouvez-vous peut-être nous parcourir les étapes clés, et peut-être ce que les clients devraient envisager, à quelque étape qu'ils se trouvent ?

21
00:03:48.980 --> 00:03:59.529
Julien Ducloy : Ouais, absolument. Le cycle de vie nous donne une structure pour comprendre l'exposition cyber dans l'industrie minière. Donc, nous commençons par l'exploration.

22
00:03:59.530 --> 00:04:06.239
Julien Ducloy : C'est une étape que les gens ne considèrent pas toujours comme exposée à la cyber, mais les données d'exploration sont incroyablement précieuses.

23
00:04:06.240 --> 00:04:21.120
Julien Ducloy : Quand on pense à tout ce qui est investi dans l'exploration, l'accès non autorisé aux données d'acquisition de site ou au système SIG pourrait coûter à une entreprise un avantage concurrentiel valant des milliards. Et ils pourraient ne jamais le savoir, en fait.

24
00:04:21.120 --> 00:04:33.079
Julien Ducloy : Et après, si on regarde l'étape suivante, la préparation du site et l'extraction, l'extraction, désolé, le risque se déplace vers la technologie opérationnelle.

25
00:04:33.080 --> 00:04:49.870
Julien Ducloy : Le système de contrôle qui aide pour les équipements de terrassement, le GPS et les systèmes de gestion de flotte. Les attaquants qui obtiennent l'accès ici peuvent causer des perturbations physiques directes et créer des risques pour la sécurité des travailleurs.

26
00:04:49.890 --> 00:04:50.570
Julien Ducloy : Non.

27
00:04:51.110 --> 00:05:04.430
Raul Munoz : Ouais, je veux dire, la sécurité, c'est énorme, et je suppose que cela nous amène à peut-être l'étape suivante, qui est le traitement. C'est probablement souvent l'un des systèmes les plus complexes, je suppose, dans le complexe minier.

28
00:05:05.360 --> 00:05:20.950
Julien Ducloy : Ouais, exactement. Le traitement serait la cible de valeur la plus élevée, et les attaques par rançongiciel contre les systèmes de traitement peuvent arrêter complètement la production. Et parfois pendant, disons, un minimum de 4 jours, des semaines ou des mois.

29
00:05:20.950 --> 00:05:34.689
Julien Ducloy : Et toute perturbation d'un système de traitement peut compromettre la qualité du produit ou créer des dommages physiques, avec des pertes financières toujours importantes.

30
00:05:34.850 --> 00:05:44.619
Julien Ducloy : Donc, la combinaison au stade de l'exposition informatique et opérationnelle devient particulièrement complexe à gérer.

31
00:05:45.550 --> 00:06:04.590
Raul Munoz : D'accord, nous sommes passés de l'exploration à l'extraction au traitement et à certains des systèmes qui pourraient être affectés. Mais même après l'extraction et le traitement du minerai, il y a des risques dans le transport et les opérations commerciales, n'est-ce pas ?

32
00:06:05.390 --> 00:06:20.729
Julien Ducloy : Ouais, le système de transport est une excellente cible, et voler des informations d'expédition pour perturber la logistique, créer des risques pour la sécurité et voler le minerai qui est toujours le produit final. Ce sont d'excellentes cibles pour les attaquants.

33
00:06:20.730 --> 00:06:45.319
Julien Ducloy : Quand on pense au marketing et à l'administration générale, on tombe dans les risques cyber classiques, les transferts frauduleux, et les informations confidentielles concurrentielles, la tarification, les contrats, les données clients. Nous pouvons donc voir que les attaques auxquelles vous êtes confronté sur tout le cycle de vie sont assez larges pour de nombreuses industries.

34
00:06:46.590 --> 00:06:59.990
Raul Munoz : Alors, avec toute cette large gamme d'expositions sur le cycle de vie, comment les chefs de file du secteur minier devraient-ils commencer à construire une résilience significative dans leur organisation ?

35
00:07:01.460 --> 00:07:18.200
Julien Ducloy : Donc, vous commencez par l'identification. Ils doivent comprendre leur profil de risque spécifique. Donc, quelle est l'infrastructure, quels sont les actifs les plus précieux, et où se trouvent les lacunes de sécurité et les vulnérabilités ?

36
00:07:18.200 --> 00:07:26.760
Julien Ducloy : Donc, et puis, à la fin, quand nous regardons la combinaison de l'actif et des lacunes de sécurité, quel est l'impact financier potentiel d'un incident ?

37
00:07:26.760 --> 00:07:44.390
Julien Ducloy : Donc, vous ne pouvez pas protéger tout également, vous voulez donc prioriser, et pour cela, la quantification de l'impact financier est critique, et c'est ce qui vous attire l'attention au niveau de la gestion, au niveau de la direction.

38
00:07:45.960 --> 00:07:56.370
Raul Munoz : D'accord ? Maintenant, le guide entre dans beaucoup de détails en ce qui concerne le contrôle de l'hygiène cyber, spécifiquement 12 d'entre eux.

39
00:07:56.480 --> 00:08:03.470
Raul Munoz : Pourriez-vous peut-être souligner ce que vous pensez être certaines des étapes les plus critiques et des contrôles d'hygiène ?

40
00:08:04.300 --> 00:08:09.659
Julien Ducloy : Bien sûr, et je vais essayer de ne pas être trop technique, mais certains

41
00:08:12.180 --> 00:08:35.419
Julien Ducloy : Ouais, eh bien, je suppose que certains du travail résonnera avec tout le monde, comme l'authentification multifacteur. Je pense qu'à ce stade, tout le monde en a entendu parler, donc c'est... c'est parce que ce contrôle est fondamental, c'est le contrôle le plus important, et parce qu'il prévient l'accès non autorisé, comme aucun autre contrôle ne le ferait.

42
00:08:35.419 --> 00:08:47.919
Julien Ducloy : Maintenant, aussi, un contrôle très bien connu est la détection et la réaction aux points de terminaison, parce qu'il aiderait à la fois à identifier la menace directement sur les systèmes, mais aussi à commencer à la contenir.

43
00:08:48.640 --> 00:09:02.780
Julien Ducloy : Et si nous regardons l'autre extrémité du spectre, après qu'un problème s'est produit, des sauvegardes sécurisées et testées. C'est donc absolument critique, c'est généralement comme votre dernier.

44
00:09:02.780 --> 00:09:13.730
Julien Ducloy : la dernière chose qui vous empêche potentiellement de payer une rançon. Et donc ce n'est pas seulement d'avoir des sauvegardes, mais aussi de tester régulièrement si nous pouvons réellement restaurer à partir d'elles.

45
00:09:13.730 --> 00:09:19.790
Julien Ducloy : Et l'efficacité de cela. Et enfin, je vais mentionner la gestion des correctifs et des vulnérabilités.

46
00:09:19.790 --> 00:09:36.110
Julien Ducloy : Garder les systèmes à jour est basique, mais c'est difficile, et en raison de toutes les contraintes de production, c'est souvent là que les attaquants trouvent leur chemin à travers les systèmes avec les systèmes non correctifs.

47
00:09:36.440 --> 00:09:37.380
Julien Ducloy : Et,

48
00:09:37.380 --> 00:09:56.729
Julien Ducloy : Cette partie s'aggrave en fait avec les puissants modèles d'IA capables en cyber. C'est donc quelque chose qui est maintenant vraiment au cœur de la discussion sur l'amélioration de la sécurité, en raison des dernières capacités d'IA en cyber.

49
00:09:57.030 --> 00:10:01.140
Raul Munoz : Ouais, c'est incroyable la vitesse à laquelle... à laquelle cela se développe.

50
00:10:01.240 --> 00:10:15.509
Raul Munoz : Maintenant, nous sommes à une phase où ce n'est pas seulement un problème informatique, et c'est quand cela devient une dimension de politique d'entreprise, n'est-ce pas ?

51
00:10:16.670 --> 00:10:33.939
Julien Ducloy : Ouais, c'est vraiment important, nous voyons cela depuis 5 ou 10 ans maintenant, et je pense que les organisations le comprennent maintenant, mais la résilience cyber nécessite l'adhésion de tous les départements. Opérations, ressources humaines, finances, juridique, et la direction générale.

52
00:10:33.940 --> 00:10:56.520
Julien Ducloy : une politique à l'échelle de l'entreprise définirait les rôles et les responsabilités de chaque équipe, et ces politiques doivent être opérationnalisées par la formation régulière et une forte coordination entre la sécurité informatique et opérationnelle. C'est vraiment la clé, parce que les attaquants autrement s'échapperaient par les fissures entre l'informatique et l'opérationnel. C'est ce que nous voyons.

53
00:10:56.540 --> 00:11:11.640
Julien Ducloy : Par exemple, un test de phishing qu'un employé échoue est une opportunité d'apprentissage pour lui, mais une attaque de phishing contre un employé non formé qui y succombe est une crise potentielle.

54
00:11:12.820 --> 00:11:15.600
Raul Munoz : Ouais, non, tout cela est assez critique.

55
00:11:15.800 --> 00:11:24.800
Raul Munoz : D'accord, pour conclure, une dernière pensée sur le risque cyber à nos auditeurs du secteur minier. Qu'aimeriez-vous dire ?

56
00:11:25.790 --> 00:11:26.750
Julien Ducloy : Productivité.

57
00:11:27.830 --> 00:11:37.229
Julien Ducloy : Les organisations minières sont uniquement vulnérables car elles combinent des données de valeur élevée, une technologie opérationnelle complexe, et souvent elles ont

58
00:11:37.230 --> 00:11:55.419
Julien Ducloy : des systèmes hérités plus anciens qui sont difficiles à corriger. Donc, ils ne peuvent pas attendre un incident cyber pour commencer à construire leur résilience. Ils doivent couvrir les bases et avoir des contrôles en place. Et surtout quelque chose que nous n'avons pas encore mentionné, mais un plan de réponse aux incidents documenté

59
00:11:55.420 --> 00:12:06.640
Julien Ducloy : et pratiqué. Et donc ils peuvent comprendre, en tant que groupe, les implications financières potentielles, avant d'avoir besoin de les expliquer aux investisseurs, ce qui dans le pire des cas.

60
00:12:07.890 --> 00:12:27.730
Raul Munoz : Ouais, merci beaucoup, Julien. C'est une vraiment importante conversation, et comme vous l'avez suggéré plus tôt, une qui devient beaucoup plus critique avec certains des progrès technologiques. J'apprécie vraiment vos perspectives. Un rappel à nos spectateurs, le Guide de résilience est disponible sur marsh.com.

61
00:12:27.940 --> 00:12:47.410
Raul Munoz : Et dans notre prochain et dernier épisode, nous nous tournons vers un défi qui est probablement à l'avant-plan de l'esprit de chacun dans tous les secteurs, mais particulièrement dans l'industrie minière, et c'est vos gens. J'espère donc que vous nous rejoindrez la prochaine fois. Merci, Dave. Merci, Julien, et à bientôt.