

Cybersécurité : les 5 questions que les industriels doivent se poser

Sécurité

Posté par : JPilo

Publié le : 1/3/2023 13:00:00

La convergence entre systèmes d'information d'entreprise et industriels (IT/OT) fait beaucoup parler d'elle ces derniers temps. La technologie occupe depuis longtemps une place clé dans ce secteur. Néanmoins, les systèmes d'automatisation et de contrôle industriels (ICS) ont été volontairement des systèmes d'information d'entreprise.

Pendant longtemps, ces domaines ont fonctionné indépendamment l'un de l'autre, la grande diversité des compétences et de technologies utilisées créant une barrière naturelle entre les deux.

La crainte de perturber les activités des organisations a entraîné l'adoption d'approches cloisonnées afin de protéger les usines, et a engendré une réticence quant à tout changement au niveau des technologies liées aux outils d'exploitation. Pire, les silos fonctionnels ont souvent donné lieu à des relations fragiles entre ingénieurs de production et équipes informatiques.

Mais ces dernières années, tout a changé. L'industrie 4.0, la connectivité à Internet, et l'introduction d'objets connectés classiques et industriels ont changé la donne.

Les environnements industriels sont de plus en plus souvent connectés à des environnements informatiques d'entreprise, et les deux domaines sont désormais intimement connectés et interdépendants. La bonne nouvelle, c'est que la suppression de ces barrières va permettre aux entreprises de gagner en efficacité, et de mieux maîtriser les risques.

Les industriels envisageant de moderniser leur parc industriel doivent cependant se poser les questions suivantes, dicit Tom Molden, DSI, Global Executive Engagement chez Tanium

1. Avons-nous bien identifié tous les actifs en présence ?

Il est de notoriété publique que nul ne peut gérer ce dont il ignore l'existence ; or, dans le monde d'aujourd'hui, il est impossible de protéger ce qu'on ne voit pas.

Les processus d'inventaire des actifs traditionnels comportaient des étapes manuelles, et reposaient fortement sur des feuilles de calcul. Nombre des nouveaux actifs introduits progressivement dans les usines sont alors passés sous les radars.

Dans le pire des cas, les équipes de production se contentaient de débrancher un appareil lorsqu'il fallait le scanner, puis de le rebrancher une fois l'opération terminée. Ainsi, pendant des années, des informations obsolètes et incomplètes ont été acceptées parce qu'il était plus important de se focaliser sur les éléments soutenant la continuité d'activité.

Mais aujourd'hui, les DSI et directeurs de production sont conscients de la valeur de la visibilité en temps réel, et de l'importance d'une vue simplifiée et complète sur les actifs technologiques d'entreprise et industriels.

2. Notre parc industriel est-il géré et protégé de façon globale ?

Dans l'industrie, il y a essentiellement deux types de technologies. Les systèmes de contrôle industriels sont divisés en plusieurs couches, telles que définies par le modèle Purdue et la norme de cybersécurité ISA/IEC 62443 IACS. Sur le plan de la gestion des actifs, il existe une distinction majeure entre les types d'appareils et le niveau d'expertise nécessaire pour les gérer.

Les deux couches inférieures de la pile regroupent des équipements effectuant généralement des tâches répétitives à haut volume, en usine comme dans le cadre plus global d'une activité industrielle. Ainsi, les capteurs et autres mécanismes doivent afficher une efficacité élevée, et ne tolèrent aucun temps d'arrêt.

Sur le plan technique, ces appareils tournent généralement sur des systèmes d'exploitation temps réel (RTOS), des systèmes propriétaires conçus et gérés par des fournisseurs de systèmes de contrôle industriel. Ces dernières années, nous avons vu émerger des fournisseurs de solutions de sécurité des systèmes industriels spécialisés dans l'évaluation et la gestion des risques pour ces types d'équipements.

En effet, avec l'essor de l'Industrie 4.0, la prolifération des équipements connectés à Internet (IoT/IIoT) au sein de ces environnements a rendu leur surface d'attaque plus étendue et difficile à gérer.

Dans l'autre moitié de la pile figurent des appareils servant généralement à contrôler les équipements des couches basses, afin de fournir des fonctions de gestion prioritaires, et de communiquer avec les systèmes d'entreprise.

Ces appareils tournent généralement sur des systèmes d'exploitation standards, comme Windows et Linux, et nécessitent les mêmes types de gestion et de contrôle que les systèmes d'une entreprise classique. Il existe également une couche d'équipements de passerelle qui s'assurent de la traduction des protocoles du niveau inférieur au niveau supérieur.

Ces derniers utilisent souvent des versions simplifiées et embarquées de systèmes d'exploitation standards. En raison de leur connectivité aux environnements d'entreprise, tous ces éléments représentent le principal vecteur de cyberattaque et de risques de sécurité. Ainsi, pour la première fois depuis des années, l'industrie a été plus ciblée que le secteur des services financiers.

Pour veiller à gérer et protéger leurs environnements de production de bout en bout, les ingénieurs, équipes informatiques et de sécurité collaborent pour mettre en place des Centres Opérationnels de Sécurité des systèmes d'information (SOC) et des processus unifiés.

L'objectif de ces coopérations est d'alimenter leurs bases de données de gestion des configurations (CMDB), leurs systèmes de gestion des informations et des événements de sécurité (SIEM) et les plateformes de gestion des workflows en données issues des meilleures sources possible.

3. Nos actifs les plus critiques sont-ils équipés des derniers correctifs ?

La plupart des professionnels de l'informatique et de la sécurité reconnaissent que la meilleure façon de se protéger des cybermenaces est de veiller à ce que les ordinateurs restent à jour.

L'observation des règles de cyberhygiène les plus strictes permet également d'augmenter le temps de fonctionnement des systèmes, et de réduire les efforts investis en

maintenance et en r solution de probl mes. Les  quipes des centres de support peuvent alors se concentrer sur des t ches plus pr cieuses.

La m me r gle s applique au milieu industriel : les  « actifs g r s   » mentionn s ci-dessus ont autant besoin de correctifs que ceux pr sents en entreprise. Il convient donc de tout mettre en  uvre pour  tendre ces bonnes pratiques en mati re de correctifs   l environnement industriel, en s appuyant id alement sur la m me plateforme que pour les actifs informatiques.

D exp rience, nous savons que cela n est pas chose facile. Les syst mes d exploitation obsol tes, les fen tres de changement restrictives, les caract ristiques techniques limit es et la segmentation des r seaux constituent g n ralement des d fis pour la gestion des correctifs dans ces environnements.

N anmoins, gr ce aux progr s technologiques r cents et   une collaboration accrue, les  quipes charg es des technologies industrielles sont toujours plus   m me d en augmenter l op rabilit  et de r duire les risques sans affecter la production.

Sur la question de la gestion des vuln rabilit s : l identification et la hi rarchisation des failles aident   focaliser l application des correctifs l  o ¹ les risques sont les plus  lev s. Par cons quent, en g rant votre programme d di  depuis la m me plateforme que celle utilis e pour identifier et hi rarchiser les vuln rabilit s, vous pourrez  viter les opportunit s d intervention manqu es, obtenir de meilleurs r sultats, et augmenter consid rablement votre productivit .

Quant aux actifs  « non g r s   » des couches inf rieures, ils sont de plus en plus menac s par des cyberattaques. Certaines entreprises se sp cialisent donc dans l identification et l analyse des vuln rabilit s dans ce domaine, et il est recommand  d agr ger des donn es issues de leurs syst mes et des v tres sur une plateforme unifiant CMDB, SIEM et gestion des workflows.

4. Sommes-nous suffisamment pr ts pour faire face   un incident ?

Pas besoin de chercher  perdument des conseils sur ce sujet. Compte tenu de la recrudescence des attaques de ransomware, d innombrables organisations proposent leurs meilleures pratiques, solutions et services.

Pour commencer, il convient de mettre en place un plan de r ponse aux incidents, et celui-ci doit couvrir les syst mes industriels. Le conseil d administration et autres cadres dirigeants doivent  tre conscients de leurs r les.

Enfin, il est n cessaire de se mettre d accord sur l entit  responsable en dernier ressort, et de d terminer les mesures   prendre pour un maximum de sc narios. Paieriez-vous la ran on en cas d attaque ? Pouvez-vous restaurer votre activit    l aide de sauvegardes, et si oui, de combien de temps avez-vous besoin ?

Si vous avez r fl chi aux implications de diff rentes attaques potentielles, votre entreprise se remettra plus rapidement sur pied. Les tests et simulations sont d excellentes fa ons de s assurer que toutes les parties prenantes sont au courant des cons quences, et suffisamment pr par es.

Concernant les capacit s des syst mes, il est toujours crucial de conna tre la situation en cas d incident. Lorsque chaque minute ou seconde compte, cette visibilit  en temps r el sur l environnement poss de une importance inestimable.

Les industriels ont donc besoin d'une source de référence, et leur aptitude à prendre des mesures et à contrôler leurs actifs depuis une même plateforme peut également être un avantage au moment crucial. Les entreprises les mieux préparées savent à l'avance quelles sont leurs principales vulnérabilités, et peuvent en minimiser l'impact en s'occupant d'abord des ressources prioritaires lorsque celles-ci s'avèrent limitées.

Enfin, il y a la question du cloud. Au vu de la progression de son adoption dans l'industrie manufacturière, on peut estimer sans risque que les entreprises continueront à chercher à profiter de l'échelle et de l'efficacité de ces environnements. Or que vous en soyez dans votre migration vers le cloud, vous gagnerez à inclure des scénarios spécifiques dans votre plan de réponse aux incidents.

5. Quel est le rôle des technologies dans l'optimisation de mon efficacité opérationnelle ?

Votre hésitation à installer des correctifs sur des machines limite-t-elle votre efficacité opérationnelle et votre capacité à accroître votre rendement ?

Les équipes de production traditionnelle ont toujours été très réticentes à l'idée de toucher le moindre équipement opérationnel. Le temps de fonctionnement est la base du rendement ; or, avec la sécurité, le rendement constitue le principal indicateur clé de performance pour les responsables.

Les fenêtres de maintenance se répétant de manière rare et brève sont donc la norme, et le dicton « le mieux est l'ennemi du bien » résume toujours bien le point de vue dominant au sein de nombreuses équipes de production.

Cependant, dans le monde contemporain, cette mentalité n'est plus la bonne. Les environnements industriels regorgent de machines gérant les actifs s'occupant des tâches physiques. Certains de ces équipements ne nécessitent que peu, voire aucune intervention humaine une fois installés.

Vient ensuite la question des postes de travail et ordinateurs portables mis à disposition du personnel des usines, et qui reçoivent généralement moins d'attention que ceux des employés d'entreprise. Au-delà de leurs risques intrinsèques, ces actifs obsolètes et vulnérables ont également un impact sur l'efficacité opérationnelle.

Il suffit de réfléchir aux ressources déployées afin de « garder un œil » sur ces machines, puis aux conséquences lorsque l'un de ces équipements tombe en panne ou est victime d'un piratage. Ajoutons à cela les ressources mobilisées dans un souci de conformité réglementaire.

Outre les cadres de conformité traditionnels concernant les environnements de contrôle industriels (ex. : ISA 62443), il existe également de nombreuses exigences plus récentes relatives aux produits connectés et affectant la production industrielle (à l'image du règlement UNECE R155/156 dans le domaine de l'automobile).

Imaginez l'impact de celles-ci à l'échelle, étendues sur plusieurs usines ou activités industrielles fonctionnant indépendamment, chacune ayant son propre ensemble de ressources gérant son propre lot d'actifs obsolètes.

L'heure est venue d'aborder la gestion des technologies industrielles sous un autre angle. Avec le modèle traditionnel, les ateliers sont gérés indépendamment. Ils mènent leurs activités dans différents coins du globe, dans des circonstances variées, et grâce à des infrastructures informatiques hétérogènes. Et à ceci s'ajoutent les activités

racup res dans le cadre d acquisitions. Ce mod le est fondamentalement inefficace.

Avec les technologies disponibles aujourd hui, et en adoptant les bonnes pratiques de cyberhygi ne dans leurs usines, les organisations pourront mieux standardiser et centraliser leurs op rations. Outre l impact sur leur degr  d exposition aux risques, une telle strat gie aura  galement un effet positif sur leur rendement.

En conclusion...

L approche consistant   traiter les technologies industrielles s par ment et de fa son ind pendante est aujourd hui improductive et expose les organisations   des cyberattaques. Les syst mes obsol tes sont remis en question, toute une g n ration d ing nieurs approche de l  ge de la retraite, et il n existe aucune solution compl te de gestion et de protection des actifs.

La r ponse   toutes ces probl matiques passe en premier lieu par la visibilit . Les organisations doivent d abord unifier leurs environnements informatiques d entreprise et industriels, et profiter de la confiance issue de leur visibilit  sur leurs actifs, leur emplacement et leur statut. Elles pourront alors intervenir aux moments opportuns et  viter les processus manuels en contr lant leurs actifs depuis une plateforme unifi e.

Les entreprises adoptant une vision globale de leurs technologies industrielles et une approche int gr e reposant sur une plateforme sont de fait les mieux g r es, et disposent des environnements les mieux prot g s. Leurs SIEM, CMDB et plateformes de gestion des workflows sont aliment s   l aide de donn es des plus qualitatives et r centes provenant de leurs environnements informatiques traditionnels comme industriels.

Leur Centre Op rationnel de S curit  est unifi , et leur mise en conformit  r glementaire est fortement automatis e. Enfin, le fait d avoir fait de l efficience op rationnelle leur objectif ultime leur permettra de prendre l ascendant sur la concurrence dans les ann es   venir.