CybersÃ©curitÃ© : les 5 questions que les industriels doivent se poser
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 1/3/2023 13:00:00

La convergence entre systÃ¨mes dâ□□information dâ□□entreprise et industriels (IT/OT) fait beaucoup parler dâ□□elle ces derniers temps. La technologie occupe depuis longtemps une place clÃ© dans ce secteur. NÃ©anmoins, les systÃ¨mes dâ□□automatisation et de contrÃ´le industriels (ICS) ont Ã©voluÃ© diffÃ©remment des systÃ¨mes dâ□□information dâ□□entreprise.

Pendant longtemps, ces domaines ont fonctionnÃ© indÃ©pendamment lâ□□un de lâ□□autre, la grande diversitÃ© des compÃ©tences et de technologies utilisÃ©es crÃ©ant une barriÃ¨re naturelle entre les deux.

La crainte de perturber les activitÃ©s des organisations a entraÃ®nÃ© lâ□□adoption dâ□□approches cloisonnÃ©es afin de protÃ©ger les usines, et a engendrÃ© une rÃ©ticence quant Ã tout changement au niveau des technologies liÃ©es aux outils dâ□□exploitation. Pire, les silos fonctionnels ont souvent donnÃ© lieu Ã des relations fragiles entre ingÃ©nieurs de production et Ã©quipes informatiques.

Mais ces derniÃ¨res annÃ©es, tout a changÃ©. Lâ□□industrie 4.0, la connectivitÃ© Ã Internet, et lâ□□introduction dâ□□objets connectÃ©s classiques et industriels ont changÃ© la donne.

Les environnements industriels sont de plus en plus souvent connectÃ©s Ã des environnements informatiques dâ□□entreprise, et les deux domaines sont dÃ©sormais intimement connectÃ©s et interdÃ©pendants. La bonne nouvelle, câ□□est que la suppression de ces barriÃ¨res va permettre aux entreprises de gagner en efficience, et de mieux maÃ®triser les risques.

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

1. Avons-nous bien identifiÃ© tous les actifs en prÃ©sence ?

Il est de notoriÃ©tÃ© publique que nul ne peut gÃ©rer ce dont il ignore lâ□□existence ; or, dans le monde dâ□□aujourdâ□□hui, il est impossible de protÃ©ger ce quâ□□on ne voit pas.

Les processus dâ□□inventaire des actifs traditionnels comportaient des Ã©tapes manuelles, et reposaient fortement sur des feuilles de calcul. Nombre des nouveaux actifs introduits progressivement dans les usines sont alors passÃ©s sous les radars.

Dans le pire des cas, les Ã©quipes de production se contentaient de dÃ©brancher un appareil lorsquâ□□il fallait le scanner, puis de le rebrancher une fois lâ□□opÃ©ration terminÃ©e. Ainsi, pendant des annÃ©es, des informations obsolÃ¨tes et incomplÃ¨tes ont Ã©tÃ© acceptÃ©es parce quâ□□il Ã©tait plus important de se focaliser sur les Ã©lÃ©ments soutenant la continuitÃ© dâ□□activitÃ©.

Mais aujourdâ□□hui, les DSI et directeurs de production sont conscients de la valeur de la visibilitÃ© en temps rÃ©el, et de lâ□□importance dâ□□une vue simplifiÃ©e et complÃ¨te sur les actifs technologiques dâ□□entreprise et industriels.

2. Notre parc industriel est-il gÃ©rÃ© et protÃ©gÃ© de faÃ§on globale ?

Dans lâ□□industrie, il y a essentiellement deux types de technologies. Les systÃ¨mes de contrÃ´le industriels sont divisÃ©s en plusieurs couches, telles que dÃ©finies par le modÃ¨le Purdue et la norme de cybersÃ©curitÃ© ISA/IEC 62443 IACS. Sur le plan de la gestion des actifs, il existe une distinction majeure entre les types dâ□□appareils et le niveau dâ□□expertise nÃ©cessaire pour les gÃ©rer.

Les deux couches infÃ©rieures de la pile regroupent des Ã©quipements effectuant gÃ©nÃ©ralement des tÃ¢ches rÃ©pÃ©titives Ã haut volume, en usine comme dans le cadre plus global dâ□□une activitÃ© industrielle. Ainsi, les capteurs et autres mÃ©canismes doivent afficher une efficience Ã©levÃ©e, et ne tolÃ¨rent aucun temps dâ□□arrÃªt.

Sur le plan technique, ces appareils tournent gÃ©nÃ©ralement sur des systÃ¨mes dâ□□exploitation temps rÃ©el (RTOS), des systÃ¨mes propriÃ©taires conÃ§us et gÃ©rÃ©s par des fournisseurs de systÃ¨mes de contrÃ´le industriel. Ces derniÃ¨res annÃ©es, nous avons vu Ã©merger des fournisseurs de solutions de sÃ©curitÃ© des systÃ¨mes industriels spÃ©cialisÃ©s dans lâ□□Ã©valuation et la gestion des risques pour ces types dâ□□Ã©quipements.

En effet, avec lâ□□essor de lâ□□Industrie 4.0, la prolifÃ©ration des Ã©quipements connectÃ©s Ã Internet (IoT/IIoT) au sein de ces environnements a rendu leur surface dâ□□attaque plus Ã©tendue et difficile Ã gÃ©rer.

Dans lâ□□autre moitiÃ© de la pile figurent des appareils servant gÃ©nÃ©ralement Ã contrÃ´ler les Ã©quipements des couches basses, afin de fournir des fonctions de gestion prioritaires, et de communiquer avec les systÃ¨mes dâ□□entreprise.

Ces appareils tournent gÃ©nÃ©ralement sur des systÃ¨mes dâ□□exploitation standards, comme Windows et Linux, et nÃ©cessitent les mÃªmes types de gestion et de contrÃ´le que les systÃ¨mes dâ□□une entreprise classique. Il existe Ã©galement une couche dâ□□Â« Ã©quipements de passerelle Â» qui sâ□□assurent de la traduction des protocoles du niveau infÃ©rieur au niveau supÃ©rieur.

Ces derniers utilisent souvent des versions simplifiÃ©es et embarquÃ©es de systÃ¨mes dâ□□exploitation standards. En raison de leur connectivitÃ© aux environnements dâ□□entreprises, tous ces Ã©lÃ©ments reprÃ©sentent le principal vecteur de cyberattaque et de risques de sÃ©curitÃ©. Ainsi, pour la premiÃ¨re fois depuis des annÃ©es, lâ□□industrie a Ã©tÃ© plus ciblÃ©e que le secteur des services financiers.

Pour veiller Ã gÃ©rer et protÃ©ger leurs environnements de production de bout en bout, les ingÃ©nieurs, Ã©quipes informatiques et de sÃ©curitÃ© collaborent pour mettre en place des Centre OpÃ©rationnel de SÃ©curitÃ© des systÃ¨mes dâ□□information (SOC) et des processus unifiÃ©s.

Lâ□□objectif de ces coopÃ©rations est dâ□□alimenter leurs bases de donnÃ©es de gestion des configurations (CMDB), leurs systÃ¨mes de gestion des informations et des Ã©vÃ©nements de sÃ©curitÃ© (SIEM) et les plateformes de gestion des workflows en donnÃ©es issues des meilleures sources possible.

3. Nos actifs les plus critiques sont-ils Ã©quipÃ©s des derniers correctifs ?

La plupart des professionnels de lâ□□informatique et de la sÃ©curitÃ© reconnaissent que la meilleure faÃ§on de se protÃ©ger des cybermenaces est de veiller Ã ce que les ordinateurs restent Ã jour.

Lâ□□observation des rÃ¨gles de cyberhygiÃ¨ne les plus strictes permet Ã©galement dâ□□augmenter le temps de fonctionnement des systÃ¨mes, et de rÃ©duire les efforts investis en

maintenance et en rÃ©solution de problÃ¨mes. Les Ã©quipes des centres de support peuvent alors se concentrer sur des tÃ¢ches plus prÃ©cieuses.

La mÃªme rÃ¨gle sâ□□applique au milieu industriel : les Â« actifs gÃ©rÃ©s Â» mentionnÃ©s ci-dessus ont autant besoin de correctifs que ceux prÃ©sents en entreprise. Il convient donc de tout mettre en Å□uvre pour Ã©tendre ces bonnes pratiques en matiÃ¨re de correctifs Ã lâ□□environnement industriel, en sâ□□appuyant idÃ©alement sur la mÃªme plateforme que pour les actifs informatiques.

Dâ□□expÃ©rience, nous savons que cela nâ□□est pas chose facile. Les systÃ¨mes dâ□□exploitation obsolÃ¨tes, les fenÃªtres de changement restrictives, les caractÃ©ristiques techniques limitÃ©es et la segmentation des rÃ©seaux constituent gÃ©nÃ©ralement des dÃ©fis pour la gestion des correctifs dans ces environnements.

NÃ©anmoins, grÃ¢ce aux progrÃ¨s technologiques rÃ©cents et Ã une collaboration accrue, les Ã©quipes chargÃ©es des technologies industrielles sont toujours plus Ã mÃªme dâ□□en augmenter lâ□□opÃ©rabilitÃ© et de rÃ©duire les risques sans affecter la production.

Sur la question de la gestion des vulnÃ©rabilitÃ©s : lâ□□identification et la hiÃ©rarchisation des failles aident Ã focaliser lâ□□application des correctifs lÃ oÃ¹ les risques sont les plus Ã©levÃ©s. Par consÃ©quent, en gÃ©rant votre programme dÃ©diÃ© depuis la mÃªme plateforme que celle utilisÃ©e pour identifier et hiÃ©rarchiser les vulnÃ©rabilitÃ©s, vous pourrez Ã©viter les opportunitÃ©s dâ□□intervention manquÃ©es, obtenir de meilleurs rÃ©sultats, et augmenter considÃ©rablement votre productivitÃ©.

Quant aux actifs Â« non gÃ©rÃ©s Â» des couches infÃ©rieures, ils sont de plus en plus menacÃ©s par des cyberattaques. Certaines entreprises se spÃ©cialisent donc dans lâ□□identification et lâ□□analyse des vulnÃ©rabilitÃ©s dans ce domaine, et il est recommandÃ© dâ□□agrÃ©ger des donnÃ©es issues de leurs systÃ¨mes et des vÃ´tres sur une plateforme unifiant CMDB, SIEM et gestion des workflows.

4. Sommes-nous suffisamment prÃªts pour faire face Ã un incident ?

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

Pour commencer, il convient de mettre en place un plan de rÃ©ponse aux incidents, et celui-ci doit couvrir les systÃ¨mes industriels. Le conseil dâ□□administration et autres cadres dirigeants doivent Ãªtre conscients de leurs rÃ´les.

Enfin, il est nÃ©cessaire de se mettre dâ□□accord sur lâ□□entitÃ© responsable en dernier ressort, et de dÃ©terminer les mesures Ã prendre pour un maximum de scÃ©narios. Paierez-vous la rançon en cas dâ□□attaque ? Pouvez-vous restaurer votre activitÃ© Ã lâ□□aide de sauvegardes, et si oui, de combien de temps avez-vous besoin ?

Si vous avez rÃ©flÃ©chi aux implications de diffÃ©rentes attaques potentielles, votre entreprise se remettra plus rapidement sur pied. Les tests et simulations sont dâ□□excellentes faÃ§ons de sâ□□assurer que toutes les parties prenantes sont au courant des consÃ©quences, et suffisamment prÃ©parÃ©es.

Concernant les capacitÃ©s des systÃ¨mes, il est toujours crucial de connaÃ®tre la situation en cas dâ□□incident. Lorsque chaque minute ou seconde compte, cette visibilitÃ© en temps rÃ©el sur lâ□□environnement possÃ¨de une importance inestimable.

Les industriels ont donc besoin dâ□□une source de rÃ©fÃ©rence, et leur aptitude Ã prendre des mesures et Ã contrÃ´ler leurs actifs depuis une mÃªme plateforme peut Ã©galement Ãªtre un Ã©norme avantage au moment crucial. Les entreprises les mieux prÃ©parÃ©es savent Ã lâ□□avance quelles sont leurs principales vulnÃ©rabilitÃ©s, et peuvent en minimiser lâ□□impact en sâ□□occupant dâ□□abord des ressources prioritaires lorsque celles-ci sâ□□avÃ¨rent limitÃ©es.

Enfin, il y a la question du cloud. Au vu de la progression de son adoption dans lâ□□industrie manufacturiÃ¨re, on peut estimer sans risque que les entreprises continueront Ã chercher Ã profiter de lâ□□Ã©chelle et de lâ□□efficience de ces environnements. OÃ¹ que vous en soyez dans votre migration vers le cloud, vous gagnerez Ã inclure des scÃ©narios spÃ©cifiques dans votre plan de rÃ©ponse aux incidents.

5. Quel est le rÃ´le des technologies dans lâ□□optimisation de mon efficience opÃ©rationnelle ?

Votre hÃ©sitation Ã dâ□□installer des correctifs sur des machines limite-t-elle votre efficience opÃ©rationnelle et votre capacitÃ© Ã accroÃ®tre votre rendement ?

Les Ã©quipes de production traditionnelle ont toujours Ã©tÃ© rÃ©ticentes Ã lâ□□idÃ©e de toucher le moindre Ã©quipement opÃ©rationnel. Le temps de fonctionnement est la base du rendement ; or, avec la sÃ»retÃ©, le rendement constitue le principal indicateur clÃ© de performance pour les responsables.

Les fenÃªtres de maintenance se rÃ©pÃ©tant de maniÃ¨re rare et brÃ¨ve sont donc la norme, et le dicton Â« le mieux est lâ□□ennemi du bien Â» rÃ©sume toujours bien le point de vue dominant au sein de nombreuses Ã©quipes de production.

Cependant, dans le monde contemporain, cette mentalitÃ© nâ□□est plus la bonne. Les environnements industriels regorgent de machines gÃ©rant les actifs sâ□□occupant des tÃ¢ches physiques. Certains de ces Ã©quipements ne nÃ©cessitent que peu, voire aucune intervention humaine une fois installÃ©s.

Vient ensuite la question des postes de travail et ordinateurs portables mis Ã disposition du personnel des usines, et qui reÃ§oivent gÃ©nÃ©ralement moins dâ□□attention que ceux des employÃ©s dâ□□entreprise. Au-delÃ de leurs risques intrinsÃ¨ques, ces actifs obsolÃ¨tes et nÃ©gligÃ©s ont Ã©galement un impact sur lâ□□efficience opÃ©rationnelle.

Il suffit de rÃ©flÃ©chir aux ressources dÃ©ployÃ©es afin de Â« garder un Å□il Â» sur ces machines, puis aux consÃ©quences lorsque lâ□□un de ces Ã©quipements tombe en panne oÃ¹ est victime dâ□□un piratage. Ajoutons Ã cela les ressources mobilisÃ©es dans un souci de conformitÃ© rÃ©glementaire.

Outre les cadres de conformitÃ© traditionnels concernant les environnements de contrÃ´le industriels (ex. : ISA 62443), il existe Ã©galement de nombreuses exigences plus rÃ©centes relatives aux produits connectÃ©s et affectant la production industrielle (Ã lâ□□image du rÃ¨glement UNECE R155/156 dans le domaine de lâ□□automobile).

Imaginez lâ□□impact de celles-ci Ã lâ□□Ã©chelle, Ã©tendues sur plusieurs usines ou activitÃ©s industrielles fonctionnant indÃ©pendamment, chacune ayant son propre ensemble de ressources gÃ©rant son propre lot dâ□□actifs obsolÃ¨tes.

Lâ□□heure est venue dâ□□aborder la gestion des technologies industrielles sous un autre angle. Avec le modÃ¨le traditionnel, les ateliers sont gÃ©rÃ©s indÃ©pendamment. Ils mÃ¨nent leurs activitÃ©s dans diffÃ©rents coins du globe, dans des circonstances variÃ©es, et grÃ¢ce Ã des infrastructures informatiques hÃ©tÃ©rogÃ¨nes. Et Ã ceci sâ□□ajoutent les activitÃ©s

rÃ©cupÃ©rÃ©es dans le cadre dâ□□acquisitions. Ce modÃ¨le est fondamentalement inefficace.

Avec les technologies disponibles aujourdâ□□hui, et en adoptant les bonnes pratiques de cyberhygiÃ¨ne dans leurs usines, les organisations pourront mieux standardiser et centraliser leurs opÃ©rations. Outre lâ□□impact sur leur degrÃ© dâ□□exposition aux risques, une telle stratÃ©gie aura Ã©galement un effet positif sur leur rendement.

En conclusion...

Lâ□□approche consistant Ã traiter les technologies industrielles sÃ©parÃ©ment et de faÃ§on indÃ©pendante est aujourdâ□□hui improductive et expose les organisations Ã des cyberattaques. Les systÃ¨mes obsolÃ¨tes sont remis en question, toute une gÃ©nÃ©ration dâ□□ingÃ©nieurs approche de lâ□□Ã¢ge de la retraite, et il nâ□□existe aucune solution complÃ¨te de gestion et de protection des actifs.

La rÃ©ponse Ã toutes ces problÃ©matiques passe en premier lieu par la visibilitÃ©. Les organisations doivent dâ□□abord unifier leurs environnements informatiques dâ□□entreprise et industriels, et profiter de la confiance issue de leur visibilitÃ© sur leurs actifs, leur emplacement et leur statut. Elles pourront alors intervenir aux moments opportuns et Ã©viter les processus manuels en contrÃ´lant leurs actifs depuis une plateforme unifiÃ©e.

Les entreprises adoptant une vision globale de leurs technologies industrielles et une approche intÃ©grÃ©e reposant sur une plateforme sont de fait les mieux gÃ©rÃ©es, et disposent des environnements les mieux protÃ©gÃ©s. Leurs SIEM, CMDB et plateformes de gestion des workflows sont alimentÃ©s Ã lâ□□aide de donnÃ©es des plus qualitatives et rÃ©centes provenant de leurs environnements informatiques traditionnels comme industriels.

Leur Centre OpÃ©rationnel de SÃ©curitÃ© est unifiÃ©, et leur mise en conformitÃ© rÃ©glementaire est fortement automatisÃ©e. Enfin, le fait dâ□□avoir fait de lâ□□efficience opÃ©rationnelle leur objectif ultime leur permettra de prendre lâ□□ascendant sur la concurrence dans les annÃ©es Ã venir.