6.4. Comment protéger vos actifs contre la cybercriminalité ?

Si l'année écoulée appris une chose, c'est que la cybercriminalité sera assurément un centre d'intérêt en 2020. Chez l'équipementier aéronautique Asco, les dégâts d'une cyberattaque s'élèvent à plusieurs millions. Les cybercriminels ont également paralysé les serveurs et les systèmes de communications mondiaux de l'entreprise d'automatisation Pilz et du fabricant de machines à tisser Picanol, pour ne citer que ces trois exemples. Les grands acteurs industriels deviennent eux aussi des victimes et voient leur production prise en otage. Comment protéger nos actifs ? (Par Valérie Couplez).

La cybersécurité doit être la priorité absolue pour toutes les entreprises. Tout a à voir avec notre soif de digitalisation. En 2020, il y aura 31 milliards d'appareils IoT. Connecter la technologie permet de récolter d'énormes avantages pour dynamiser la productivité, la qualité et l'efficience, ou développer des nouveaux services. Dans le domaine de la maintenance, c'est précisément cela qui va permettre de passer à la maintenance prédictive. Un grand pas en avant donc, mais qui comporte des risques. A l'inverse de la technologie informatique (IT), les commandes classiques ne sont pas cybersécurisées. « Le monde de la technologie d'exploitation (OT) a toujours été un des circuits fermés dans l'atelier de production. Pas de regards indiscrets pour les curieux. Aujourd'hui, on connecte les machines et les systèmes entre eux, avec le monde extérieur et le cloud à un rythme effréné, ce qui n'est pas sans risques », explique Mirel Sehic, global director of Cybersecurity chez Honeywell Building Solutions.

Sensibiliser davantage

Pilz en a fait la triste expérience l'année dernière. Le 13 octobre, les systèmes de surveillance des serveurs web de Pilz détectent une activité suspecte. Dès le lancement la cyberattaque, Pilz désactive tous les réseaux et les serveurs de l'entreprise, tant en interne que vers l'extérieur pour éviter l'escalade. Les pirates ont cependant réussi à introduire un cheval de Troie, ou ransomware, au niveau du serveur mondial et à coder une partie des données. Susanne Kunsher, managing partner : « La vague d'attaques contre nous et d'autres entreprises montre clairement que la cybercriminalité devient une menace sérieuse pour la paix et la prospérité de notre pays. Il faut fournir de grands efforts pour veiller à ce que ce type de criminalité organisée soit mieux connue et que les entreprises, les organisations, le gouvernement et, le politique puissent collaborer plus étroitement dans le futur afin d'éviter que d'autres entreprises et organisations vivent ce que nous avons vécu. »

65% de failles de sécurité en plus

D'après une étude du cabinet de conseil Gartner, 20% des organisations disposants de réseaux IoT ont déjà subi au moins une attaque liée à IoT. Le nombre de failles de sécurité a augmenté de 65% au cours des cinq dernières années. Des chiffres alarmants qui doivent inquiéter les entreprises. Heinz-Uwe Gernhard, spécialiste IT Security and Application chez Robert Bosch et responsable du groupe de sécurité à la VDMA, résume le problème : « J'aime bien comparer cela avec des véhicules motorisés. Les premiers chauffeurs dans les années '20 du siècle dernier avaient une toute autre conscience du danger que les chauffeurs d'aujourd'hui. Actuellement, on accorde moins d'attention aux éléments du fait de l'intégration de divers systèmes. Les véhicules d'aujourd'hui rendent la conduite plus sûre que jadis. Les risques liés à l'IT sont du niveau de la période de 1920. Les utilisateurs doivent y accorder une grande attention et il faut de nombreuses connaissances pour garantir la cybersécurité. Une plus grande prise de conscience des dangers est donc la première étape. »

La cybersécurité est une affaire de personnes

« Pour pouvoir garantir une disponibilité élevée des machines et l'intégrité des données à tous les niveaux pendant le cycle de vie complet d'un actif, les fournisseurs de solutions d'automatisation et de machines doivent créer de l'interaction avec l'opérateur, lequel doit être conscient du risque permanent de cyberattaques.

Des mesures de précaution fondamentales doivent être prises au niveau de l'opérateur pour déployer une cyber-résistance et réduire l'impact d'un cyberattaque », explique Steffen Zimmermann, de l'Industrial Security Competence Center du VDMA. Chaque entreprise, chaque machine, chaque système est en principe une victime potentielle. « La cybersécurité est une histoire de personnes » poursuit Mire ! Sehic. « Avant d'examiner les processus et la technologie, II faut sensibiliser les collaborateurs aux risques et leur inculquer les bonnes instructions de cybersécurité pour chaque tâche, sans bloquer leur travail. » Néanmoins, le risque restera élevé pour certaines applications. « Nous parlons de 'risk appetite'. Un aéroport sera plus dans la ligne de mire qu'un hôtel. Au plus le chiffre de cyberattaque est élevé, au plus il faut prévoir de sécurité pour atténuer les risques. Mais nous ne serons jamais complètement en sécurité », souligne Mirel Sehic.

Augmenter les investissements

Pour limiter les cyber-risques, les entreprises vont devoir ouvrir le porte-monnaie. D'après Gartner, le montant dédié à la sécurité IoT en 2021 va doubler pour atteindre 1,9 milliards d'euros. Une plus grande attention va être accordée à la cybersécurité OT et un budget sera consacré à l'amélioration de l'hygiène digitale fondamentale et à l'état d'alerte en cas incident. Heinz-Uwe Gernhard : « Tout cela doit avoir lieu au niveau du management. C'est là que les risques liés aux réseaux doivent être identifiés et pesés pour ensuite définir les mesures appropriées. En ce qui concerne la disponibilité de la technologie de production, le management doit se faire une idée des conséquences pouvant découler d'un incident et ce que cela coûtera. Suite à l'interconnectivité mondiale aujourd'hui, personne n'est à l'abri d'une cyberattaque. » L'investissement dans une cybersécurité sera négligeable par rapport à l'impact d'une cyber-attaque.

Comment déployer une cyber-protection

A quoi doit ressembler une cyber-protection ? Cela dépend des environnements de production. Néanmoins, il y a un fil conducteur une cybersécurité doit avoir plusieurs couches, tel un oignon, pour protéger correctement les actifs. Mirel Sehic : « Il n'est pas possible d'exclure tous les risques mais on peut mettre en place une stratégie efficiente pour exclure les cyber-risques autant que possible. Le noyau est constitué de routines simples mais efficaces : la mise en place d'un pare-feu pour les connexions sortantes, l'implémentation de nouveaux patches pour les systèmes et les applications et la formation des collaborateurs à une hygiène de sécurité fondamentale. Pour la couche de sécurité tout autour, on part d'une mesure zéro. Où en est votre entreprise ? Quels sont les risques ? Sur base des réponses, la sécurité sera étendue avec l'implémentation d'une surveillance là où se trouvent les plus gros risques. Il faut aussi prévoir une stratégie performante pour la gestion des usb. La solution de cybersécurité est alors déployée, couche par couche. La dernière couche a trait à l'état d'alerte lors d'un incident. Que faire si une cyberattaque se produit ? Tous les collaborateurs doivent connaître la bonne procédure et des copies de sauvegarde s'avèrent utiles. Testez régulièrement le fonctionnement des back-ups et conservez un back-up hors ligne. »

www.maintenance-magazine.be – Mars 2020