CYBERATTAQUES

Quelles conséquences sur la sécurité en entreprise ?

Alors que le numérique est désormais présent dans la plupart des domaines d'activité, les entreprises sont devenues des cibles de choix pour les cybercriminels. Si la majorité des attaques visent à extorquer de l'argent, d'autres, plus ciblées, notamment sur des installations industrielles, n'ont comme autre objectif que de dégrader l'appareil productif ou d'empêcher son fonctionnement. Des actions malveillantes qui posent question sur le plan de la sécurité des opérateurs.

***BOÎTE NOIRE*, FILM** sorti en septembre dernier au cinéma, raconte l'enquête de l'aviation civile sur le crash d'un avion qui – attention *spoiler* – s'avèrera avoir été causé par un hackeur entré dans le système informatique de l'appareil. Résultat, plus de 300 morts dont 12 membres d'équipage. Cette histoire est une fiction, mais elle illustre un problème potentiel qui touche une très grande partie des entreprises dans le monde : les cyberattaques. Un sujet qui concerne à la fois la sécurité de l'outil industriel mais aussi celle des personnels.

Dans son rapport d'activité 2020, l'Agence nationale de la sécurité des systèmes informatiques (ANSSI) rapporte une multiplication par quatre de ces types d'attaques. Si sur près de 2 287 signalements, seuls 759 concernaient de vrais incidents, la menace est considérée suffisamment sérieuse pour que le gouvernement décide, en février 2021, de mobiliser un milliard d'euros pour renforcer les dispositifs de cybersécurité et aider les entreprises à mieux se défendre. Ces dernières, avec la numérisation croissante des activités professionnelles et un recours massif aux services à distance, sont devenues d'autant plus exposées au risque de cyberattaques.

La majorité des actions malveillantes ne sont réalisées, *a priori*, que dans un but lucratif grâce à des *ransomwares* – ou rançongiciels – qui bloquent les systèmes de l'entreprise ciblée, qui n'a plus qu'à payer les malfaiteurs et espérer que ces derniers cessent leur emprise… Ces attaques ont été particulièrement médiatisées lors de la pandémie de Covid-19 lorsque des hôpitaux, comme celui d'Oloron-Sainte-Marie dans les Pyrénées-Atlantiques, ont été victimes de rançongiciels. Les malfaiteurs exigeaient 50 000 dollars en échange du déblocage du système, et l'accès aux données des patients et au stock de médicaments a été fortement perturbé.

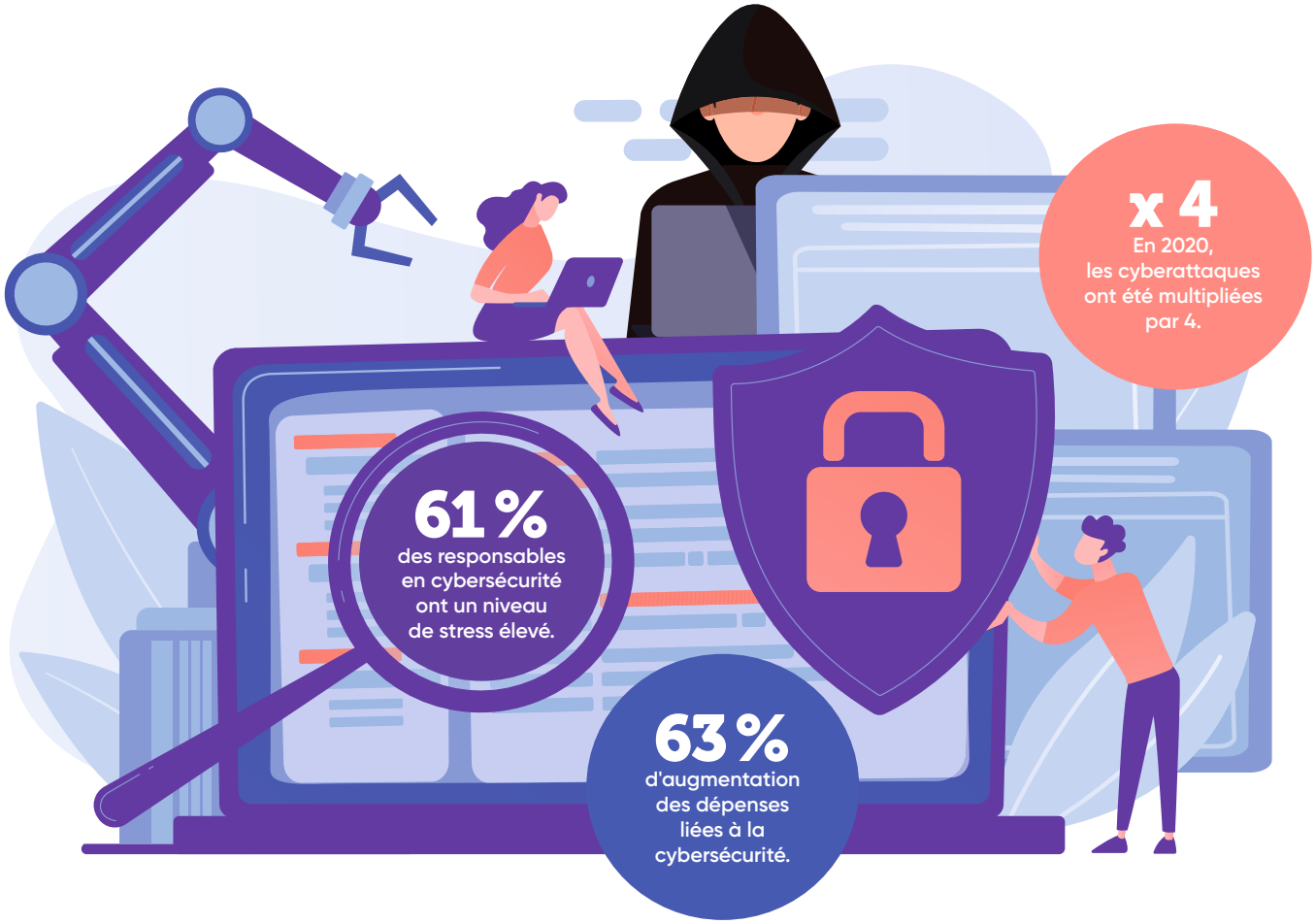
« *C'est un peu la partie immergée de l'iceberg*, explique Pascal Lamy, responsable d'études à l'INRS et auteur d'un article sur le sujet dans la revue *Hygiène & Sécurité du Travail* . *Ces attaques sont réalisées pour extorquer de l'argent mais conduisent souvent à une forte perturbation, voire à l'arrêt total, de l'activité de l'entreprise ou de l'organisme ciblé. Selon les dysfonctions créées, cela peut induire un certain nombre de risques directs ou indirects pour les personnes.* » En témoigne, de façon tragique, le décès d'une patiente à l'hôpital universitaire de Düsseldorf en septembre 2020, cette dernière n'ayant pu être prise en charge en urgence par l'hôpital dont le système informatique était paralysé par une cyberattaque.

Quand le risque machine rencontre le risque cyber

« *La littérature disponible sur le sujet ne mentionne que très rarement les impacts humains à la suite d'une cyberattaque*, explique Hélène Courtecuisse, fondatrice de Lisis conseil, consultante en cybersécurité et membre du Clusif (association de promotion de la cybersécurité, réunissant entreprises et administrations autour du développement des bonnes pratiques pour la sécurité du numérique). *Les entreprises ou organismes n'aiment pas communiquer sur ce sujet, mais l'ampleur de certaines attaques ne peut être passé sous silence et alerte sur les risques potentiels…* » Ainsi, en 2010, une aciérie allemande est victime d'une cyberattaque visant à perturber gravement ses hauts fourneaux, ce qui aurait pu causer un accident industriel majeur. Autre exemple, en 2017, le groupe Saint-Gobain touché par une cyberattaque doit arrêter le fonctionnement de son haut fourneau et fonctionner en mode dégradé.

À noter également, l'existence de certains *malwares* qui visent directement les automates de sécurité Schneider Electric censés protéger les installations industrielles : « *Ici, il y a une possibilité de conséquences humaines graves en rendant inopérant les systèmes de sécurité* », précise François Massé, ingénieur sûreté de fonctionnement à l'Ineris. Ces attaques d'ampleur restent assez exceptionnelles et si certains *malwares* utilisés commencent à être bien connus : Stuxnet, Wannacry, Triton…, de nouvelles vulnérabilités et façons de les exploiter apparaissent sans cesse.

« *Une culture sécurité se développe concernant les systèmes de contrôle industriels par exemple, les*



© Designed by vectorjuice/Freepik/Vecteezy.com

fabricants communiquent sur les failles potentielles et apportent des correctifs, explique David Michel, directeur activité nucléaire chez ISOIngénierie, entreprise spécialisée dans la sécurité industrielle. *Concernant la prévention de ce risque, le mieux est encore de faire le lien avec la sécurité fonctionnelle historique en lui ajoutant la dimension cyber.* »

C'est en suivant ce raisonnement que l'on comprend tout le défi que représente le risque cyber en termes de prévention, selon Nino Di Renzo, responsable de la sécurité des systèmes d'information (RSSI) à l'INRS : « *Ce qui change drastiquement, c'est la surface d'attaque*, explique l'informaticien. *Auparavant, on avait une machine-outil qui n'était pas raccordée au réseau. Cette dernière pouvait avoir des défaillances techniques, un risque modéré par de la maintenance préventive, par exemple. Mettez cette machine sur un réseau, l'enjeu change complètement. L'exposition au risque devient d'autant plus importante qu'elle est moins identifiable ; comment savoir qu'une machine est contrôlée à distance, de façon malveillante ? Cela est d'autant plus vrai que les entreprises sont bien moins protégées contre le risque cyber. De nombreuses TPE et PME ne sont pas du tout à jour en matière de protection numérique de leurs équipements.* »

Sécuriser les systèmes informatiques pour protéger… les opérateurs

Et même lorsque certaines entreprises investissent beaucoup pour se défendre des cyberattaques, une simple défaillance ou une inattention peut mettre à mal tous leurs efforts. Pour exemple, cette société qui, quelques jours après avoir déployé son nouveau système de sécurité, s'est vue attaquée *via*… une machine à café connectée – non sécurisée – branchée par les salariés dans leur salle de pause. « *Certaines histoires peuvent paraître anecdotiques mais toutes alertent sur nos lacunes en matière de cybersécurité*, explique Alexandre Depriester, autre RSSI à l'INRS. *Il y a un manque flagrant de prise en compte du risque cyber en milieu professionnel : compte tenu de l'augmentation massive des attaques, si le danger pour les opérateurs est représenté aujourd'hui comme à la marge par rapport au coût financier ou à l'impact sur l'outil productif, cette vision des choses entraînera nécessairement des blessés demain.* »

Afin d'éviter que l'usine 4.0 ne se transforme en cauchemar, tous les spécialistes du sujet recommandent de s'intéresser dès aujourd'hui à la protection des systèmes informatiques, mais aussi d'interroger les besoins réels de connexion, comme l'indique Nino Di Renzo : « *Lorsque l'on possède une ligne de production, il faut vraiment étudier l'intérêt de connecter celle-ci au réseau Internet en se demandant ce qu'il y a à gagner* ». En effet, pour des questions de maintenance, ou de gestion à distance, les dirigeants d'entreprise sont poussés à toujours plus d'intégration réseau : « *Une action qui ne doit pas être réalisée à la légère* », selon Hélène Courtecuisse, qui invite chaque décisionnaire à bien s'entourer de ressources en interne, ou à faire appel à une aide extérieure, afin de concevoir une infrastructure réseau solide et sécurisée. Un réseau qu'il s'agira ensuite de maintenir à jour, puisque, tout comme la prévention, la sécurité informatique n'est jamais acquise. ■

Lucien Fauvernier

En savoir plus

■ « SÉCURITÉ des machines : le "risque cyber" comme risque émergent ? », article paru dans la revue *Hygiène & Sécurité du Travail* n° 256, septembre 2019, réf. NT 76.

À télécharger sur www.inrs.fr