Real Humans : quand les robots deviennent les bras armés des criminels

Depuis l'Antiquité, les hommes ont imaginé des êtres artificiels capables de reproduire le travail humain ; du mythe de Pygmalion avec Galatée, en passant par Léonard de Vinci, qui au XVe siècle proposait déjà des croquis d'un robot, jusqu'aux XXe siècle, où l'idée de robot s'est concrétisée. Les Hommes ont alimenté les fantasmes et les craintes d'une machine qui prendrait le dessus sur l'homme. De nombreuses oeuvres littéraires et cinématographiques ont ainsi vu le jour autour de ce sujet.

Au début des années 2010, la série Real Humans débarque sur les petits écrans. Son action se déroule dans une Suède contemporaine alternative, où des androïdes appelés « hubots » - contraction de « humains » et « robots » - investissent maisons et entreprises pour accomplir des tâches répétitives, comme les tâches ménagères ou le travail à la chaîne.

Si ce synopsis semble futuriste, il ne s'éloigne finalement pas beaucoup de ce que de nombreuses organisations ont déployé ces dernières années, à l'instar de l'Automatisation des Processus Robotiques, ou RPA (Robot Process Automation en anglais), une technologie qui consiste à automatiser les processus métier en s'appuyant sur des robots logiciels ou de l'intelligence artificielle. Elle permet la répétition programmée d'actions humaines à faible valeur ajoutée, telles que le traitement d'emails, les chatbots ou encore la gestion de commande.

Dans la fiction comme dans la réalité, hubots et RPA ont été créés dans le même but : gagner du temps, tout en réduisant les coûts de main d'oeuvre et en minimisant le risque d'erreurs humaines. Les procédures redondantes et chronophages pour les humains sont réduites, voire éliminées. Hubots et RPA partagent cependant aussi des risques similaires.

En effet, si les hubots sont certes pratiques, la série met en évidence les menaces sous-jacentes qu'ils représentent. Ils ont notamment accès à des foyers ou des entreprises, et sont dotés d'une force hors du commun. En outre, bien qu'ils soient programmés pour obéir uniquement à des personnes prédéterminées, leur absence de conscience fait qu'il n'ont pas de notion de bien ou de mal, et se contentent d'exécuter les ordres reçus. Grâce à eux, leurs propriétaires peuvent donc contourner la loi, mais aussi des criminels, en modifiant le code informatique qui régit leurs actions. Il est facile de détourner les hubots, puisque ces derniers bénéficient d'un port USB au niveau de leur cou, permettant de les connecter à un ordinateur pour les programmer. Donc, à moins de se pencher en détails sur leur code, impossible de déterminer à première vue si un hubot est compromis.

Il est aisé de faire un ici un parallèle avec le RPA, puisque ce dernier agrandit de manière conséquente la surface d'attaque dans le réseau, en raison du manque de surveillance des activités des robots ainsi que du partage ou de la réutilisation des identifiants nécessaires pour s'y connecter. De plus, Les paramètres sont aisément modifiables, puisque les identifiants sont stockés dans des fichiers ou bases de données, généralement mal sécurisés. Les cybercriminels peuvent par conséquent compromettre ces robots, et s'en servir comme porte d'entrée vers le réseau de l'entreprise et les données sensibles. Si les organisations ne surveillent pas étroitement les activités des RPA, il est impossible de différencier un robot standard d'un compromis.

Qu'il s'agisse des hubots ou du RPA, il est primordial de se pencher sur les risques associés et de

faire son possible pour les contenir et protéger ses actifs, ou données, les plus précieux. Dans la seconde saison de Real Humans, le spectateur voit des hubots développer une liberté de pensée et s'émanciper progressivement de « leurs » humains, qui se retrouvent parfois dépassés. Dans la vie réelle, pour maintenir le contrôle du RPA tout en tirant parti de ses avantages, les organisations doivent tout d'abord considérer les RPA comme des accès à privilèges, et doivent par conséquent surveiller leurs activités étroitement afin de détecter toute action inhabituelle ou suspecte, partage d'identifiant, ou encore pratique à risque. En outre, la mise en place d'un coffre-fort numérique permet de protéger les identifiants ; ainsi lorsque les robots les demandent auprès du stockage local, le serveur central les récupère alors dans le coffre-fort, permettant d'effectuer les tâches en toute sécurité. Enfin, en cas de compromission d'un identifiant, les entreprises doivent absolument rendre le changement régulier des mots de passe obligatoire, via par exemple un système de rotation automatique, pour simplifier les processus.

A en croire les romans, ou encore les fictions développées pour les grands et petits écrans, le quotidien des particuliers et professionnels sera bientôt envahi de robots ; et la fascination des auteurs pour le côté obscur de ces machines les pousse le plus souvent à en montrer les travers et dangers pour la société. Or, correctement déployée et gérée, la robotisation apporte des bénéfices, tels qu'une productivité accrue et moins d'erreurs opérationnelles, et donc une source de compétitivité non négligeable pour les entreprises. Les organisations empruntant le chemin de l'innovation ont donc besoin d'adopter une approche de cybersécurité adéquate, tout en sensibilisant régulièrement leurs équipes aux bonnes pratiques. Alors, elles pourront réellement faire leur entrée dans le futur, sans craindre d'être dépassées par leurs propres machines !