Un nouveau rapport de GoSecure révèle un décalage entre la perception et la réalité vis-à-vis des priorités de cybersécurit

Les principaux vecteurs d'attaque identifiés par les testeurs d'intrusion ne sont pas perçus par les professionnels de cybersécurité comme étant des éléments essentiels contribuant à la maturité du niveau de sécurité de leur organisation

Montréal, QC., le 16 juillet 2020— GoSecure, un fournisseur de services de détection et réponse gérées (MDR et de plateforme de détection et réponse pour les terminaux (EDR) , a publié aujourd'hui un nouveau rapport de recherche. Intitulé « Distinction entre les perceptions sur la cybersécurité et la réalité », ce rapport révèle un décalage entre les perceptions des défenseurs sur comment protéger au mieux leur organisation, ce qui a été mis en place et ce qui est nécessaire selon les constats réels des testeurs d'intrusion de GoSecure.

« Ce rapport illustre ce que les professionnels de cybersécurité perçoivent comme étant important pour le niveau de maturité général de sécurité d'une organisation », a déclaré Neal Creighton, CEO de GoSecure. « Il souligne également que la réalité, par rapport à ce qui est mis en place, peut être considérablement différente. Les perceptions quant à qui est important s'alignent adéquatement pour se défendre vis-à-vis des techniques d'attaques majoritairement connues utilisées par les testeurs d'intrusion. Cependant, notre équipe de piratage éthique continue d'identifier des contrôles manquants ou des constats critiques en lien avec chaque point du sondage ».

Pour faire la distinction entre la perception et la réalité, l'équipe de recherche de GoSecure a développé un « sondage », en collaboration avec Serene-risc, un réseau mobilisé de connaissances en cybersécurité. Le sondage se concentrait sur l'importance de mesures ou de contrôles de sécurité spécifiques et s'ils étaient implantés au sein de leur organisation. Les mesures de sécurité identifiées dans le sondage incluaient l'authentification à facteurs multiples, les politiques relatives aux mots de passe, les mesures de sécurité spécifiques, la gestion des mises à jour, les fonctionnalités activées par défaut, l'inventaire des actifs, et la visibilité sur les terminaux. Les résultats du sondage ont été recoupées les constats de l'équipe de piratage éthique de GoSecure.

Les résultats principaux comprennent :

- **L'authentification à facteurs multiples (MFA)** est prisée par les professionnels de sécurité;93% des répondants ont noté le MFA comme étant « important » ou « très important ». Malheureusement, seulement 47% ont complètement intégré le MFA au sein de leur organisation et 13% n'ont mis aucun MFA en place. L'équipe de test d'intrusion de GoSecure a indiqué que le MFA était un contrôle de sécurité manquant dans 36% de ses mandats.

- **Les politiques relatives aux mots de passe** sont bien établies, mais présentent des complexités variées. Les mots de passe d'une longueur de plus de six caractères sont supportés par 56,3% des répondants et 74,8% ont répondu que les mots de passe doivent être composés d'une combinaison de lettres, de chiffres et de caractères spéciaux. Toutefois, le point de vue sur les exigences de changements réguliers de mots de passe est mitigé avec 43,7% déclarant que c'est important contre 43,7% pensant le contraire. Étonnamment, 40% des répondants n'ont pas, ou ont partiellement, mis en place leur perception de politique de mots de passe idéale. Même avec toutes ces réponses sur les politiques de mots de passe et leurs complexités, les testeurs d'intrusion de GoSecure réussissent à cracker des mots de passe dans 25% des cas en utilisant la pulvérisation de mots de passe, une technique relativement élémentaire pour cracker des mots de passe.

- **La gestion des mises à jour** est notée comme « important » ou « très important » par 90% des répondants. En réalité toutefois, 52,6% ont indiqué que cela prenait des semaines, des mois, voire des années pour appliquer les correctifs et mises à jour appropriés. Selon l'expérience de l'équipe de piratage éthique de GoSecure, l'application des correctifs et mises à jour Windows est généralement bien gérée, notamment grâce à l'abondance d'outils gratuits disponibles. Toutefois, cela n'est pas le cas pour le reste des applications utilisées dans le cadre des affaires courantes. Des applications cruciales, telles que Java, Flash, ou des navigateurs n'appartenant pas à Microsoft, sont généralement moins bien maintenus et sont à l'origine de nombreuses vulnérabilités.

De manière générale, le rapport conclut que malgré le fait qu'il y ait des efforts concertés dans l'industrie pour protéger les systèmes, il existe encore de multiples lacunes qui ne sont pas considérées par les organisations. En plus de souligner les décalages, le rapport présente des conseils pratiques et des pistes d'actions réalisables provenant des testeurs de GoSecure pour remédier aux écarts et lacunes de sécurité révélées par la recherche.

« Les équipes de sécurité sont constamment sous pression et, tel qu'illustré par ce rapport, il est parfois possible de passer à côté de simples changements à mettre en place ». Enchaîné par Creighton : « en tant que membres de la communauté de cybersécurité, nous sommes fiers d'offrir des pistes d'actions et des recommandations réalisables. Chaque petite étape améliore progressivement le niveau de maturité d'une organisation qui, ultimement, est nécessaire pour rester en avance sur les adversaires d'aujourd'hui ».

À propos de GoSecure

GoSecure est reconnu comme étant un leader et un innovateur en ce qui a trait aux solutions de cybersécurité. L'organisation est la première – et la seule – à intégrer la détection de menaces pour les terminaux, les réseaux et les services messagerie au sein d'un seul service de détection et réponse gérées. La plateforme de détection et réponse livre une détection prédictive multi-vecteurs, une prévention et une réponse en appliquant une combinaison unique d'analyse comportement, d'investigation « forensics » de

mémoire, d'apprentissage automatique et de techniques de réputation pour contrer les menaces les plus avancées. Nos services MDR sont dirigés par des niveaux de services agressifs pour une réponse rapide et des services de mitigation active qui touchent directement les réseaux et terminaux de nos clients. Ensemble, ces capacités offrent la meilleure réponse face à l'augmentation accrue de la sophistication et de l'évolution des logiciels malveillants et des employés malicieux qui ciblent les personnes, les processus et les systèmes. En mettant l'accent sur l'innovation, la qualité, le respect et l'intégrité, GoSecure est devenu un fournisseur de produits et services de cybersécurité reconnu pour des organisations de toutes tailles et évoluant dans tout type d'industrie.