Protéger son entreprise contre les ransomwares : un enjeu de Direction générale

Le recours massif au digital de la part des entreprises pour mener à bien leurs opérations les ont amenées à faire évoluer leur mode de gestion, à stocker et échanger toujours plus d'informations directement sur et depuis leurs postes de travail. C'est ce changement de paradigme qui explique en partie le succès et la montée en puissance des cyberattaques ces dernières années, notamment celles réalisées via des Ransomwares qui exigent de leurs victimes une rançon pour débloquer leurs systèmes ou ne pas publier leurs données confidentielles. Ces attaques ciblent en priorité les utilisateurs lors de leur interaction avec Internet (site web ou mail piégé) pour la compromission initiale, avant de contaminer le reste du système d'information de l'entreprise par des mouvements latéraux.

On notera d'ailleurs à ce sujet que la filière criminelle des ransomwares s'est structurée : sur le Darknet, il existe des acteurs qui éditent des kits prêts à l'emploi et proposent à la location des plateformes de contrôle, ainsi que des prestataires de blanchiment d'argent pour les rançons payées en cryptomonnaie. Ils permettent ainsi à des commanditaires de lancer très rapidement leurs premières attaques avec peu de connaissances techniques. Ce phénomène n'est plus anecdotique, son modèle d'affaires très rentable évolue (on parle maintenant de triple extorsion) et représente un marché de plusieurs centaines de millions d'euros chaque année à l'échelle mondiale, avec même un début de réaction au niveau des États.

Traiter le sujet avant d'être touché

L'analyse des attaques (publiées) sur les trois dernières années montre que les organisations de toute taille et de tout secteur sont concernées : des TPE locales aux multinationales. Le sujet doit être pris au sérieux par toutes les entreprises et intégré dans leur gouvernance (pas uniquement au niveau de la DSI, mais plutôt des Directions générales qui joueront un rôle fondamental de sponsor pour la réussite du projet). Cette prise de conscience réalisée, il faut ensuite évaluer comment faire. À ce stade, nombre d'entreprises limitent leur réponse à une question d'outillage, souvent coûteux. Si cette approche peut dans une certaine mesure être efficace, elle n'est clairement pas suffisante notamment lorsque la promesse d'une sécurisation automatique et sans effort est claironnée.

Focus sur le maillon faible

Concrètement, c'est l'articulation utilisateur/poste de travail qui est le maillon clé à prendre en considération. Dès lors, le sujet de la sensibilisation est incontournable et doit faire partie dès le début du projet d'un pan important du dispositif. Cette action fondatrice permettra aux équipes d'intégrer des connaissances et d'adopter de bons réflexes sur l'utilisation de l'outil informatique et de la messagerie électronique en particulier. Pour autant, il est aussi nécessaire d'évaluer la configuration desdits postes de travail. En ce sens, sur des postes ciblés et représentatifs, il est

nécessaire de réaliser un « Stress Test ».

Cette approche consiste à fournir une évaluation à un moment précis, pour un compte utilisateur et un ordinateur donné, de son exposition et de sa résistance aux vecteurs d'attaques des groupes de ransomwares actifs, c'est-à-dire leurs Techniques, Tactiques et Procédures (TTPs). Parmi les thématiques évaluées, nous pouvons notamment citer des points structurants comme : les droits des utilisateurs, les mises à jour logicielles (pas seulement celles de Windows, mais également celles des applications tierces), le cloisonnement du réseau, la sécurité des applications, le filtrage de contenu des emails et de la navigation web, la journalisation pertinente des événements, la détection des événements suspects, la stratégie de sauvegarde des données telle qu'elle est réellement effectuée et telle qu'elle est comprise par les utilisateurs, ou encore le niveau de préparation aux incidents de sécurité et la sensibilisation des collaborateurs.

Vérifier et améliorer son niveau de résistance contre les Ransomwares est donc un sujet stratégique pour l'ensemble des entreprises. C'est en se mobilisant à large échelle et en actualisant en permanence sa posture qu'il sera possible de limiter son exposition au cyber risque.

Stéphane REYTAN
Directeur BlueTrusty – une marque ITS Group