ProtÃ©ger des ransomwares : un enjeu de Direction gÃ©nÃ©rale
Internet
PostÃ© par : JulieM
PubliÃ©e le : 16/6/2021 13:00:00

Le recours massif au digital de la part des entreprises pour mener Ã bien leurs opÃ©rations les ont amenÃ©es Ã faire Ã©voluer leur mode de gestion, Ã stocker et Ã©changer toujours plus d'informations directement sur et depuis leurs postes de travail.

Câ□□est ce changement de paradigme qui explique en partie le succÃ¨s et la montÃ©e en puissance des cyberattaques ces derniÃ¨res annÃ©es, notamment celles rÃ©alisÃ©es via des Ransomwares qui exigent de leurs victimes une ranÃ§on pour dÃ©bloquer leurs systÃ¨mes ou ne pas publier leurs donnÃ©es confidentielles.

Ces attaques ciblent en prioritÃ© les utilisateurs lors de leur interaction avec Internet (site web ou mail piÃ©gÃ©) pour la compromission initiale, avant de contaminer le reste du systÃ¨me dâ□□information de lâ□□entreprise par des mouvements latÃ©raux.

On notera dâ□□ailleurs Ã ce sujet que la filiÃ¨re criminelle des ransomwares sâ□□est structurÃ©e : sur le Darknet, il existe des acteurs qui Ã©ditent des kits prÃªts Ã lâ□□emploi et proposent Ã la location des plateformes de contrÃ´le, ainsi que des prestataires de blanchiment dâ□□argent pour les ranÃ§ons payÃ©es en cryptomonnaie.

Ils permettent ainsi Ã des commanditaires de lancer trÃ¨s rapidement leurs premiÃ¨res attaques avec peu de connaissances techniques. Ce phÃ©nomÃ¨ne nâ□□est plus anecdotique, son modÃ¨le dâ□□affaires trÃ¨s rentable Ã©volue (on parle maintenant de triple extorsion) et reprÃ©sente un marchÃ© de plusieurs centaines de millions dâ□□euros chaque annÃ©e Ã lâ□□Ã©chelle mondiale, avec mÃªme un dÃ©but de rÃ©action au niveau des Ã□tats.

Traiter le sujet avant dâ□□Ãªtre touchÃ©

Lâ□□analyse des attaques (publiÃ©es) sur les trois derniÃ¨res annÃ©es montre que les organisations de toute taille et de tout secteur sont concernÃ©es : des TPE locales aux multinationales. Le sujet doit Ãªtre pris au sÃ©rieux par toutes les entreprises et intÃ©grÃ© dans leur gouvernance (pas uniquement au niveau de la DSI, mais plutÃ´t des Directions gÃ©nÃ©rales qui joueront un rÃ´le fondamental de sponsor pour la rÃ©ussite du projet).

Cette prise de conscience rÃ©alisÃ©e, il faut ensuite Ã©valuer comment faire. Ã□ ce stade, nombre dâ□□entreprises limitent leur rÃ©ponse Ã une question dâ□□outillage, souvent coÃ»teux. Si cette approche peut dans une certaine mesure Ãªtre efficace, elle nâ□□est clairement pas suffisante notamment lorsque la promesse dâ□□une sÃ©curisation automatique et sans effort est claironnÃ©e.

Focus sur le maillon faible

ConcrÃ¨tement, câ□□est lâ□□articulation utilisateur/poste de travail qui est le maillon clÃ© Ã prendre en considÃ©ration. DÃ¨s lors, le sujet de la sensibilisation est incontournable et doit faire partie dÃ¨s le dÃ©but du projet dâ□□un pan important du dispositif.

Cette action fondatrice permettra aux Ã©quipes dâ□□intÃ©grer des connaissances et dâ□□adopter de bons rÃ©flexes sur lâ□□utilisation de lâ□□outil informatique et de la messagerie Ã©lectronique en particulier. Pour autant, il est aussi nÃ©cessaire dâ□□Ã©valuer la configuration desdits postes de travail. En ce sens, sur des postes ciblÃ©s et reprÃ©sentatifs, il est nÃ©cessaire de rÃ©aliser un

Â« Stress Test Â».

Cette approche consiste Ã fournir une Ã©valuation Ã un moment prÃ©cis, pour un compte utilisateur et un ordinateur donnÃ©, de son exposition et de sa rÃ©sistance aux vecteurs dâ□□attaques des groupes de ransomwares actifs, c'est-Ã -dire leurs Techniques, Tactiques et ProcÃ©dures (TTPs).

Parmi les thÃ©matiques Ã©valuÃ©es, nous pouvons notamment citer des points structurants comme : les droits des utilisateurs, les mises Ã jour logicielles (pas seulement celles de Windows, mais Ã©galement celles des applications tierces), le cloisonnement du rÃ©seau, la sÃ©curitÃ© des applications, le filtrage de contenu des emails et de la navigation web, la journalisation pertinente des Ã©vÃ©nements, la dÃ©tection des Ã©vÃ©nements suspects, la stratÃ©gie de sauvegarde des donnÃ©es telle quâ□□elle est rÃ©ellement effectuÃ©e et telle quâ□□elle est comprise par les utilisateurs, ou encore le niveau de prÃ©paration aux incidents de sÃ©curitÃ© et la sensibilisation des collaborateurs.

VÃ©rifier et amÃ©liorer son niveau de rÃ©sistance contre les Ransomwares est donc un sujet stratÃ©gique pour lâ□□ensemble des entreprises. Câ□□est en se mobilisant Ã large Ã©chelle et en actualisant en permanence sa posture quâ□□il sera possible de limiter son exposition au cyber risque.

StÃ©phane REYTAN
Directeur BlueTrusty - une marque ITS Group