Ransomware : organiser sa dÃ©fense, garder la position de force
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 15/10/2021 15:00:00

Lors de la derniÃ¨re Ã©dition du Forum International de la CybersÃ©curitÃ© (FIC), lâ□□ANSSI et le ministÃ¨re de la DÃ©fense ont rappelÃ© la volontÃ© nationale de renforcer les capacitÃ©s de cybersÃ©curitÃ© franÃ§aises avec le recrutement et la formation de 5 000 cyber-combattants dâ□□ici 2025.

Une initiative visant Ã renforcer la lutte contre les cybermenaces et la recrudescence des attaques de ransomware. Ces derniÃ¨res visent de plus en plus dâ□□organismes publics franÃ§ais depuis 2020, et ont conduit Ã la paralysie de nombreuses organisations contraintes de payer une ranÃ§on sans garantie de rÃ©cupÃ©rer leurs donnÃ©es in fine.

Pour Thomas HÃ©lary, Country Manager France chez CyberArk, de nombreuses entreprises recherchent une Â« solution miracle Â» pour empÃªcher les attaques et Ã©viter de se retrouver en une des media. Or, en 2021 se protÃ©ger contre les ransomwares â□□ et les attaques rÃ©pÃ©tÃ©es, ainsi que par double ou triple extorsion qui s'ensuivent â□□ relÃ¨ve plus dâ□□une stratÃ©gie de sÃ©curitÃ©, que dâ□□un ensemble particulier d'outils.

Â« Les ransomwares sont plus rÃ©pandus et rentables que jamais auparavant, avec des attaques qui se multiplient, augmentant ainsi lâ□□inquiÃ©tude des agences de sÃ©curitÃ© du monde entier pour la sÃ©curitÃ© des organisations et des personnes.

En effet, cette activitÃ© malveillante, initialement conduite par des cybercriminels chevronnÃ©s et opportunistes, s'est transformÃ©e en une industrie souterraine gÃ©nÃ©ralisÃ©e. Aujourdâ□□hui, tout individu ayant des connaissances en informatique peut ainsi accÃ©der Ã des kits d'outils clÃ©-en-main et lancer des attaques de ransomware Ã un rythme alarmant. Or, la cybersÃ©curitÃ© est un sport dâ□□Ã©quipe.

Tous les acteurs doivent par consÃ©quent collaborer et la dÃ©fense doit Ãªtre prÃªte Ã faire face Ã tout ce que les attaquants de lâ□□adversaire leur lance. Les Ã©quipes informatiques et de sÃ©curitÃ© doivent donc anticiper lâ□□ensemble des Ã©lÃ©ments, des angles dâ□□attaques et chemins potentiels quâ□□un ransomware peut emprunter. La nÃ©cessitÃ© de "penser comme un attaquant" nâ□□a jamais Ã©tÃ© plus rÃ©elle.

Plus largement, les entreprises doivent se prÃ©parer au pire et sâ□□armer contre cette menace. Tout dâ□□abord, reformuler lâ□□ensemble de leurs hypothÃ¨ses sur les cyber-risques, en admettant quâ□□elles seront tÃ´t ou tard victimes de vols de donnÃ©es, les aidera Ã anticiper autant que possible les risques et Ã se protÃ©ger proactivement, tout en formant les employÃ©s.

De plus, rÃ©voquer les droits d'administrateur dans les environnements IT des organisations est aujourdâ□□hui indispensable, alors que les points et identifiants dâ□□accÃ¨s Ã privilÃ¨ges sont dÃ©sormais lâ□□une des principales cibles des cybercriminels.

Identifier lâ□□ensemble de ces accÃ¨s et gÃ©rer les niveaux dâ□□autorisations favorisera en effet lâ□□identification des comportements inhabituels et la rÃ©duction des risques. Pour davantage de prÃ©paration, simuler des attaques en interne favorisera une meilleure rÃ©action en cas de campagne rÃ©elle.

A lâheure oÃ¹ les cybercriminels semblent dominer le terrain, la contre-attaque se met en place au sein des entreprises et des gouvernements pour reprendre le dessus et protÃ©ger les donnÃ©es.

Si les Ã©volutions technologiques mettent les deux parties Ã armes Ã©gales, garder une longueur dâavance en adoptant lâattitude dâun cybercriminel pour se protÃ©ger permettra de rÃ©duire, voire de limiter les risques dâattaques de ransomwares, Ã long terme. Â»