Payer un rancongiciel s'expose Ã des amendes.
Internet
PostÃ© par : JulieM
PubliÃ©e le : 18/10/2021 13:00:00

Alors que les entreprises continuent dâ□□Ãªtre les cibles privilÃ©giÃ©es des cyberattaquants et quâ□□elles continuent de payer leurs ranÃ§ons afin de limiter les dÃ©gÃ¢ts, notre gouvernement tente dâ□□apporter une rÃ©ponse avec un rapport qui fait part de recommandations pour "lever les freins au dÃ©veloppement en France d'un marchÃ© mature de la cyber assurance".

L'objectif est dÃ©fini : en structurant le segment assurantiel, c'est tout l'Ã©cosystÃ¨me numÃ©rique franÃ§ais qui pourrait devenir plus robuste grÃ¢ce Ã une meilleure prÃ©vention.

Dans les grandes lignes, ce rapport parlementaire propose d'interdire aux assureurs de couvrir les ranÃ§ons. Lâ□□argument fort du gouvernement au pouvoir :Â

Â« Le paiement des ranÃ§ons alimente la cybercriminalitÃ© et rien ne garantit que la ranÃ§on payÃ©e soit un gage de retour Ã la situation initiale, explique la dÃ©putÃ©e de la Loire, ValÃ©ria Faure-Muntian (LREM).Â

Â« Le paiement encourage mÃªme les cybercriminels Ã rÃ©cidiver et en incite d'autres Ã concevoir des cyberattaques Â».

Face Ã cette situation inÃ©dite, il peut Ãªtre de bon augure de se demander sâ□□il est prÃ©fÃ©rable que les entreprises payent leurs ranÃ§ons ou non. LoÃ¯c GuÃ©zo, Directeur stratÃ©gie cybersÃ©curitÃ© SEMEA chez Proofpoint, examine cette proposition :

Â« Notre dernier rapport State of the Phish 2021 indique que 34 % des organisations ont choisi de payer les ranÃ§ons, et ce malgrÃ© les mises en garde du gouvernement sur le sujet.

Cela signifie-t-il que la plupart des victimes optent pour des solutions rapides plutÃ´t que pour un investissement Ã long terme dans la sÃ©curisation de leurs actifs numÃ©riques ?

Nous pouvons certainement spÃ©culer sur un certain nombre de facteurs qui auraient pu contraindre une organisation Ã payer une ranÃ§on en 2021.Â

Les attaquants continuent de mettre leurs cibles sous pression, les menaÃ§ant non seulement de ne pas accÃ©der aux donnÃ©es, mais aussi de les divulguer publiquement si les ranÃ§ons ne sont pas payÃ©es.

Ce deuxiÃ¨me niveau d'extorsion pourrait ainsi entacher la rÃ©putation des dÃ©cideurs dans certains cas. Et en tout Ã©tat de cause, si une organisation n'a pas anticipÃ© ou testÃ© de maniÃ¨re approfondie une rÃ©ponse Ã une infection gÃ©nÃ©ralisÃ©e par ranÃ§ongiciel, elle prend le risque dâ□□Ãªtre contrainte Ã devoir payer la ranÃ§on afin de limiter les dÃ©gÃ¢ts matÃ©riels dans un contexte dâ□□urgence.

La rÃ©action Ã une infection par un ranÃ§ongiciel est propre Ã chaque type dâ□□entreprise. L'ampleur de l'infection, l'impact sur les opÃ©rations et le montant de la ranÃ§on sont autant de facteurs susceptibles d'influencer la dÃ©cision de gestion retenue de lâ□□attaque.Â

Mais une bonne pratique est de privilÃ©gier dâ□□investir en amont sur le vecteur initial

dâ□□entrÃ©e par mail que sur la remÃ©diation et le paiement des ranÃ§ons. Â»