Ransomware et continuité d'activité

L'ANSSI a publié le 5 février 2020 son rapport sur "l'état de la menace rançongiciel à l'encontre des entreprises et institutions".

> *"Un rançongiciel est un code malveillant empêchant la victime d'accéder au contenu de ses fichiers afin de lui extorquer de l'argent"*
>
> *"Ces codes malveillants représentent actuellement la* ***menace informatique la plus sérieuse*** *pour les entreprises et institutions par le nombre d'attaques quotidiennes et leur impact potentiel sur la* ***continuité d'activité*****"**
>
> *"Les rançongiciels représentant un risque non négligeable de rupture d'activité, de nombreuses* ***assurances*** *proposent de le couvrir. Cette couverture consiste souvent en ce que l'assureur paye tout ou partie de la rançon. Des sociétés se sont développées autour de ce paiement des rançons en proposant des services de négociation avec les attaquants. Aujourd'hui, les assurances incitent les victimes à payer la rançon qui s'avère souvent moins élevée que le coût d'un rétablissement de l'activité sans le recours à la clé de déchiffrement. Pour autant cette couverture n'empêche pas les victimes d'être attaquées de nouveau. Cette incitation à payer valide le modèle économique des cybercriminels et les amène déjà à augmenter les rançons et à multiplier leurs attaques."*

Télécharger (PDF, 1.92Mo)