

### **Ransomware WannaCry : 3 leçons à tirer de l'attaque**

#### **Sécurité**

Posté par : JPilo

Publié le : 14/6/2017 14:30:00

Constituant ce jour, la cyber-attaque la plus dévastatrice de l'année 2017, l'attaque de WannaCry a eu un impact considérable sur des entreprises et des organisations du monde entier. Le programme a infecté plus de 200 000 ordinateurs dans 150 pays, paralysant tout, des hôpitaux aux entreprises de logistique.

S'il faudra encore attendre plusieurs mois avant que les enquêteurs spécialisés n'aient fait le point sur toutes les retombées, l'attaque a opportunément tiré la sonnette d'alarme sur l'importance de la sécurité dans des entreprises de tous les secteurs.

#### **Mettre à jour, mettre à jour, mettre à jour**

En théorie, l'impact du ransomware WannaCry aurait dû être minime, car Windows avait publié un correctif de vulnérabilité dès le 14 mars 2017. En réalité, au regard des estimations internes d'entreprises du secteur, il semble que seules 10 à 15 pour cent des entreprises, dans le monde, avaient installé la mise à jour critique.

La plupart des entreprises n'étaient pas protégées et ont dû répondre à l'attaque avec des correctifs d'urgence.

Ceci débouche sur notre premier enseignement important, à savoir que les chefs d'entreprises ne doivent pas sous-estimer l'importance des mises à jour de sécurité. Combien de fois avons-nous vu le service informatique devoir attendre l'approbation de la hiérarchie pour pouvoir installer des correctifs critiques pour la sécurité ?

Les directeurs financiers répuent parfois à autoriser les mises à jour lorsqu'elles exigent une indisponibilité des applications pendant une période cruciale telle que la fin d'un trimestre financier, où la moindre vente est importante.

Mais si retarder une mise à jour de sécurité peut être avantageux à court terme, comme l'a montré avec force WannaCry, cette manière de faire accroît la vulnérabilité de l'entreprise à long terme.

#### **Changez votre façon de penser la sécurité**

Aujourd'hui, les PME et les grandes entreprises adaptent leur modèle d'entreprise pour se réinventer dans cette ère de perturbation numérique. Ce même principe doit être appliqué à la gestion de la sécurité intérieure.

Investir dans la meilleure infrastructure est la base de toute stratégie de sécurité. Mais bénéficier d'un réseau sûr un jour ne signifie pas que vous pouvez vous reposer sur vos lauriers.

Une fois l'infrastructure en place, de nombreuses entreprises renouent avec la stratégie dépassée de la "réponse aux incidents". À l'ère numérique où les problèmes peuvent surgir et faire boue de neige à chaque instant, une telle pratique conduit au désastre.

Quelle est donc la stratégie à suivre ? La meilleure solution consiste à évoluer vers la

philosophie de la "réponse continue", une démarche qui passe par des investissements dans des outils et des services de détection et de prévention permettant d'avoir une vision complète du système de défense et de corriger rapidement tous les points faibles.

La voie de la mutation numérique que suivent de nombreuses entreprises offre l'opportunité de ne tirer que des avantages des nouvelles technologies numériques, mais il est important de comprendre combien la capacité à s'adapter est indispensable pour que cette stratégie fonctionne.

Il est essentiel de disposer en un clin d'œil des informations les plus actuelles sur la vulnérabilité de l'entreprise pour pouvoir prendre des décisions éclairées et améliorer la sécurité dans son ensemble.

### Faites confiance aux experts

L'émergence de logiciels de protection à une fréquence sans précédent rend aujourd'hui pratiquement impossible pour les entreprises de s'orienter seules sur le terrain miné de la sécurité.

Dans ces circonstances, il est essentiel de s'appuyer sur l'expertise d'un fournisseur de services de sécurité managés (MSSP), et ce pour deux raisons.

Tout d'abord, collaborer avec un fournisseur de sécurité peut contribuer à développer une stratégie préventive efficace.

En second lieu, un MSSP peut apporter un soutien précieux pendant les moments critiques.

Rappelons que la sécurité n'est pas une science exacte. Personne ne peut prévoir toutes les cyber-attaques, mais comme dans une partie d'échecs, la mise en place d'une bonne stratégie mettra à chaque instant toutes les chances de votre côté.

Affirme Srinivasan C.R.  Senior Vice President, Global Product Management & Data Centre Services at Tata Communications.