19 sep 2019 -12:40

Le CCB met en garde : ne laissez pas des ransomware paralyser la Belgique

Les ransomware ne cessent de proliférer mais il est possible de s'en protéger.

Qui sont les cibles des ransomware ?

Tout le monde peut être victime d'un ransomware : des joueurs de jeux en ligne, les indépendants, les hôpitaux et les grandes entreprises. En France, un ransomware a récemment mis à l'arrêt pas moins de 120 hôpitaux. Plus tôt cette année, un hôpital belge a aussi été victime. Dans son rapport annuel de 2018, l'ENISA a soulevé que le secteur de la santé était une cible privilégiée de telles attaques. Et la Belgique n'est pas en reste puisque cette année la presse a également fait état de plusieurs cas de ransomware. Mais tous ces cas ne sont que la partie visible de l'iceberg. Les particuliers qui sont victimes de telles mésaventures n'en font que rarement état et les entreprises ne sont en général pas très inclines à révéler qu'elles ont été victimes d'un ransomware. Outre les pertes financières, c'est également l'image de la société qui est touchée.

Comment vous protéger contre les ransomware ?

Bonne nouvelle : se protéger contrer les ransomware est possible.
Pour tous les internautes :
• S'il est primordial de protéger votre appareil à l'aide d'un logiciel antivirus, une protection spécifique contre les ransomware est devenue incontournable. Installez un logiciel anti-ransomware: Acronis Ransomware Protection, Kasperski Anti-Ransomware Tool for Business, McAfee Ransomware Interceptor (Pilot). Pour l'utilisateur Windows 10: Windows Defender Antivirus.
• En outre, il demeure important de reconnaître à temps les faux messages et de réaliser régulièrement des mises à jour de tous vos systèmes.
• Enfin, réalisez régulièrement une copie de sauvegarde au cas où vous deviez néanmoins être victime d'un ransomware.
Pour les entreprises et les organisations :
Les recommandations qui s'adressent à l'internaute lambda revêtent naturellement tout autant d'importance pour les entreprises et les organisations. Mais nous leur conseillons tout de même d'encore davantage se protéger.
• Il se peut que, pour les PME et les indépendants, la protection « End-point » telle que décrite précédemment s'avère suffisante. Par contre, il est recommandé aux grandes entreprises d'utiliser une solution anti-ransomware spécifique aux business.
• Prévoyez un business continuity and recovery plan assorti d'un système de sauvegarde éprouvé.
• Veillez à ce que votre organisation soit préparée en cas de cyberattaque. Jetez un œil à notre webinaire : https://www.youtube.com/watch?v=-cHcTidmT1Y&feature=youtu.be
• Demandez à un spécialiste de vérifier l'architecture and policy de votre système informatique. (en ce compris le politique en matière de patching, de formation des utilisateurs, de réseau, de segmentation du réseau, etc..)
• Élaborez une stratégie en matière de cybersécurité. Découvrez ici comment vous y prendre.

https://cyberguide.ccb.belgium.be/nl

Un ransomware, c’est quoi au juste ?

Un ransomware est un virus qui est installé sur un appareil sans que le propriétaire n’en ait donné l’autorisation. Le virus tient l’appareil en otage et les fichiers sont cryptés jusqu’à l’obtention d’une rançon.

Contact pour la presse

Katrien Eggers : 0485 765 336, katrien.eggers@cert.be

Centre pour la Cybersécurité Belgique
Rue de la Loi 16
1000 Bruxelles
Belgique
http://www.ccb.belgium.be

Andries Bomans
Responsable communication
+32 471 66 00 06
andries.bomans@ccb.belgium.be

Katrien Eggers
Responsable communication
+32 485 76 53 36
katrien.eggers@cert.be