beazley

L'explosion des cyberattaques par rançongiciels appelle une cyberdéfense à tous les niveaux

1 juillet 2021

Cet article est le premier d'une série qui traite de la cyberprévention, clé de voûte de la lutte contre les cyberattaques.

Les cyberextorsions sont aujourd'hui davantage le fait de hackers qui exploitent l'accès aux réseaux, installent des logiciels malveillants très redoutables, ciblent les sauvegardes, volent des données et menacent de révéler certaines informations. Face à ces criminels de plus en plus ingénieux et performants, les entreprises et les collectivités ont plus que jamais intérêt à adopter une approche de sécurité tous azimuts et à prendre des mesures draconiennes pour stopper net ou du moins minimiser les effets d'une cyberextorsion à tous les niveaux.

Les organisations doivent mener la vie dure aux acteurs malveillants à tout instant

La cyberextorsion est un processus et il existe plusieurs occasions tout au long de la chaîne pour disrupter les agissements des criminels. Les rançongiciels sont évitables à condition de former les collaborateurs à intervalle régulier et de manière exhaustive aux moyens de se prémunir contre cette menace évolutive. Les organisations devraient non seulement essayer de prévenir les infections par rançongiciel, mais aussi se préparer à une infection potentielle par une sécurité construite par strates successives, réduisant chacune le risque et la probabilité d'une attaque par rançongiciel. Apprendre aux collaborateurs comment reconnaître les e-mails de phishing ; instaurer des sauvegardes sécurisées off line ; encrypter les données stockées ; surveiller les intrusions réseau ; patcher sans cesse les systèmes et les applications – toutes ces actions rendent plus difficile l'exploitation des accès par les

attaquants, même si ceux-ci parviennent à s'introduire dans un réseau.

7 étapes pour se protéger contre les rançongiciels

1. **Evaluer les risques :** Pour gérer les risques, il faut d'abord les identifier : quels sont les risques, où se trouvent-ils et quelle est la gravité de leurs conséquences ?

2. **Contenu et distribution des e-mails :** Mettez en place pour tous les messages e-mail entrants des vérifications SPF (Sender Policy Framework) strictes de l'authenticité des adresses des expéditeurs. Filtrez tous les messages entrants sur des contenus malveillants, y compris des fichiers exécutables, des documents contenant des macros et des liens vers des sites malveillants.

3. **Gérer rigoureusement les accès :** Les rançongiciels ne doivent pas devenir viraux au sein d'une organisation. Pour cela, il est nécessaire de réguler de manière appropriée les accès utilisateurs et systèmes à travers l'organisation : accès privilégiés aux actifs critiques (serveurs, endpoints, applications, bases de données, etc.) et renforcement de l'utilisation de l'authentification multifactorielle (MFA) (par exemple, accès à distance/VPN, applications orientées vers l'extérieur/webmail).

4. **Sauvegarder vos systèmes et bases de données essentiels :** Instaurez des sauvegardes régulières qui sont vérifiées et stockées de manière sécurisée hors ligne. Utilisez des authentifiants de sauvegarde forts et uniques, en les sécurisant séparément. Testez les sauvegardes de manière à assurer la restauration des données.

5. **Former les utilisateurs :** La plupart des attaques reposent sur des erreurs commises par les utilisateurs. Apprenez aux utilisateurs de reconnaître les e-mails de phishing contenant des liens ou pièces jointes malveillants. Des exercices anti-phishing à intervalle régulier (à l'instar des exercices incendie) sont un excellent moyen pour augmenter la vigilance des utilisateurs.

6. **Patcher les systèmes et les applications :** Réalisez des scans de vulnérabilité réguliers et patchez au plus vite les vulnérabilités critiques au niveau des endpoints et des serveurs, en particulier lorsqu'il s'agit de systèmes orientés vers l'extérieur.

7. **Sécuriser les accès à distance :** N'exposez pas directement le protocole de bureau à distance (RDP) à Internet. Utilisez une passerelle de bureau à distance (RDG) ou sécurisez le RDP via un réseau privé virtuel (VPN) à authentification multifactorielle.

Pour en savoir plus sur l'approche 360 de Beazley en matière de rançongiciels et sa gamme de cyberservices, permettant aux entreprises d'améliorer leur protection contre les cyberattaques et donc de réduire les risques :

beazley