***Qui veut la peau de lâ□□homme cachÃ© dans les rÃ©seaux ?***
**SÃ©curitÃ©**
PostÃ© par : JulieM
PubliÃ©e le : 2/11/2016 13:30:00

Alors que dÃ©marre la saison 2 de la sÃ©rie amÃ©ricaine Mr. Robot en France, la question de la sÃ©curitÃ© des donnÃ©es reste sur toutes les bouches. Cette sÃ©rie, centrÃ©e sur le cyber-piratage, est reconnue par les experts du marchÃ© comme Ã©tant proche de la rÃ©alitÃ©. RÃ©compensÃ©e aux Emmy Awards 2016 en septembre dernier, elle aborde en effet les techniques les plus connues de piratage informatique et rÃ©veille les craintes les plus avÃ©rÃ©es des individus et des organisations en termes de cyberattaque.Â

Parmi les thÃ©matiques abordÃ©es, celle de la sÃ©curitÃ© des rÃ©seaux revient constamment, intrinsÃ¨que Ã  tout type de cyber menace. Le pirate informatique y agit toujours comme lâ□□homme invisible qui sâ□□introduit dans les systÃ¨mes insidieusement pour y exfiltrer des donnÃ©es, un classique des attaques de sÃ©curitÃ©.

MÃªme si les rÃ©sultats de la derniÃ¨re Ã©tude conduite par PwC dÃ©montrent que la part dâ□□attaques de sÃ©curitÃ© a baissÃ© de 47 % en France par rapport Ã  2015 â□□ preuve que les pratiques semblent sâ□□amÃ©liorer â□□ la nÃ©cessitÃ© de poursuivre les efforts de sÃ©curitÃ© reste une prioritÃ©.

**Pour Pascal Beurel, Directeur Technique Europe du Sud chez Gigamon, la fiction nâ□□est pas loin de la rÃ©alitÃ© et doit contribuer Ã  inciter Ã  la vigilance :**

Â« Le concept de cette sÃ©rie et sa thÃ©matique peuvent, Ã  premiÃ¨re vue, faire sourire les spÃ©cialistes de la cybersÃ©curitÃ©, pourtant en la regardant avec un deuxiÃ¨me niveau de lecture, lâ□□approche est intÃ©ressante.Â

En effet, dans la plupart des Ã©pisodes, le schÃ©ma reste le mÃªme, sâ□□introduire de maniÃ¨re illÃ©gitime et insidieuse dans les systÃ¨mes dâ□□une organisation pour y dÃ©rober des donnÃ©es, en prendre le contrÃ´le pour servir un objectif final malveillant selon les cas.Â

En regardant la sÃ©rie, on a lâ□□impression que nâ□□importe qui peut hacker un systÃ¨me. Heureusement, la rÃ©alitÃ© est tout autre, mais le message de fond est pertinent et peut inciter les organisations Ã  plus de vigilance.

Le mot dâ□□ordre est donc la connaissance complÃ¨te de son rÃ©seau, et la visibilitÃ© totale pour quâ□□aucun dÃ©tail nâ□□Ã©chappe aux Ã©quipes informatiques, parce en dÃ©finitive on ne peut pas sÃ©curiser ce quâ□□on ne voit pas, ni chasser un programme malveillant qui se cache dans le rÃ©seau.Â

Pour y parvenir, les bons outils et surtout les bonnes pratiques sont nÃ©cessaires pour lutter efficacement contre cette "menace invisible". La visibilitÃ© est indispensable Ã  la dÃ©tection de la moindre anomalie et pour permettre aux Ã©quipes de sÃ©curitÃ© de dÃ©terminer la nature du problÃ¨me. Il peut sâ□□agir par exemple dâ□□une panne technique, dâ□□une erreur humaine ou dâ□□une cyberattaque.

Cette visibilitÃ©, combinÃ©e Ã  une connaissance aussi exhaustive que possible du contexte dont elles peuvent bÃ©nÃ©ficier grÃ¢ce aux mÃ©tadonnÃ©es qui offrent un ensemble riche dâ□□informations permettent de mieux analyser un problÃ¨me. Ainsi, avec les bonnes informations envoyÃ©es aux bons outils dâ□□analytiques, les Ã©quipes IT protÃ¨gent mieux les systÃ¨mes.

Par ailleurs, avec les big data un volume grandissant de donnÃ©es sont en circulation continue sur les rÃ©seaux, ce qui peut gÃ©nÃ©rer un grand nombre de difficultÃ©s pour les entreprises. En effet, outre les pertes dâ□□informations, des pannes, des problÃ¨mes de congestion ou encore des ralentissements de la bande passante peuvent survenir.Â

Or, dans ces cas de figure, la visibilitÃ© gÃ©nÃ©rale ne permet pas aux Ã©quipes dâ□□identifier prÃ©cisÃ©ment la nature de lâ□□incident. Câ□□est pourquoi elles doivent pouvoir sÃ©lectionner le trafic de donnÃ©es de leur choix afin de lâ□□envoyer sur un outil dâ□□analyse spÃ©cifique pour lâ□□Ã©tudier et rediriger le problÃ¨me vers lâ□□Ã©quipe concernÃ©e.

De Wargames Ã  Mr. Robot, en passant par Terminator, Hacker ou Minority Report, lâ□□informatique et la cybersÃ©curitÃ© nourrissent la fiction depuis toujours ; les crÃ©ateurs cherchent Ã  se rapprocher le plus possible de la rÃ©alitÃ©.Â

Au-delÃ  du divertissement ou des controverses que de telles histoires peuvent gÃ©nÃ©rer, les experts du marchÃ© peuvent y voir une rÃ©elle opportunitÃ© dâ□□utiliser ces fictions pour poursuivre la sensibilisation aux cybermenaces. Ils aideront ainsi les organisations Ã  maÃ®triser la connaissance de leurs systÃ¨mes, de leurs rÃ©seaux, et Ã  mieux voir ce quâ□□ils veulent sÃ©curiser. Â»Â