CybersÃ©curitÃ© : Il n'y a pas d'Ã©chec et mat!
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 20/10/2017 13:30:00

Octobre est le mois de la cybersÃ©curitÃ© avec entre autres les Assises de la SÃ©curitÃ© Ã Monaco, et It-sa Ã Nuremberg, rendez-vous annuels incontournables des spÃ©cialistes du secteur, ou encore le discours annuel de lâ□□ANSSI et ses propositions dans le renforcement de la lutte contre les cybermenaces.

Â

Alors que 2017 est marquÃ©e comme lâ□□annÃ©e du ransomware, lâ□□ensemble des experts sâ□□accordent sur la nÃ©cessitÃ© dâ□□amÃ©liorer la sÃ©curitÃ© des organisations et des Etats. La Commission EuropÃ©enne (CE) a dâ□□ailleurs annoncÃ© sa volontÃ© dâ□□augmenter les moyens des pays membres de lâ□□UE pour faire face aux cyberattaques.

Elle propose notamment de renforcer l'Agence de lâ□□Union europÃ©enne chargÃ©e de la sÃ©curitÃ© des rÃ©seaux et de lâ□□information (ENISA), en crÃ©ant un cadre de certification de cybersÃ©curitÃ© Ã l'Ã©chelle de l'UE, un plan dâ□□action relatif aux modalitÃ©s de rÃ©action aux crises et incidents de grande ampleur en matiÃ¨re de cybersÃ©curitÃ©, ainsi quâ□□un Centre europÃ©en de recherche et de compÃ©tences dans ce domaine.

Jean-FranÃ§ois Pruvot, Regional Director Europe West and South Europe chez CyberArk, estime que ces initiatives sont nÃ©cessaires car lâ□□Ã©ducation seule ne suffit plus pour faire face aux menaces. Cette agence EuropÃ©enne ne peut cependant pas fonctionner sans une collaboration avec les cyber-experts du marchÃ© :

Â« Les entreprises, les Ã©diteurs et les gouvernements doivent Ãªtre les trois mousquetaires de la cybersÃ©curitÃ©, leurs expertises Ã©tant complÃ©mentaires et indispensables Ã la lutte contre les cybermenaces, face Ã un ennemi de plus en plus redoutable.

En effet, le machine learning et lâ□□intelligence artificielle contribuent Ã rendre les pirates informatiques â□□ dÃ©jÃ trÃ¨s chevronnÃ©s â□□ de plus en plus forts, et capables de rivaliser avec les experts de la cybersÃ©curitÃ©. On assiste dÃ©sormais Ã une partie dâ□□Ã©checs sans fin, oÃ¹ chaque camp cherche Ã garder un ou deux coups dâ□□avance sur lâ□□autre, car lâ□□adversaire peut causer des dÃ©gÃ¢ts aux consÃ©quences parfois irrÃ©versibles.

Ces derniÃ¨res annÃ©es, difficile de passer Ã cÃ´tÃ© des cyberattaques de grande ampleur qui ont affectÃ© de nombreuses grandes entreprises Ã intervalles rÃ©guliers, telles que les attaques ransomwares WannaCry et NotPetya avant lâ□□Ã©tÃ©. Un signe, sâ□□il en fallait, que des mesures drastiques de cyberdÃ©fense doivent Ãªtre prises et des moyens investis par les hautes autoritÃ©s, et lâ□□annonce de ces nouveaux moyens pour lâ□□ENISA par la CE est un pas essentiel dans ce sens.

Les derniÃ¨res attaques ont en effet dÃ©montrÃ© que le paysage des menaces est en constante Ã©volution, et la part dâ□□imprÃ©visible liÃ©e au renouvÃ¨lement et Ã la sophistication des mÃ©thodes des hackers est le talon dâ□□Achille des organisations. Ce quâ□□une agence peut et doit apporter est donc le cadre qui permettra aux cibles des pirates de rÃ©agir rapidement afin dâ□□avoir connaissance des risques pour mieux sâ□□en prÃ©munir et de contrer ces attaques en protÃ©geant leurs systÃ¨mes et accÃ¨s.

En outre, les entreprises ont Ã©galement vu lâ□□arrivÃ©e dâ□□hackers Ã©thiques dans leur enceinte. Ces derniers sont capables de comprendre le schÃ©ma de pensÃ©e des pirates informatiques malveillants, ainsi que leurs techniques, et sont donc plus Ã mÃªme dâ□□anticiper leurs actions. Leur prÃ©sence au sein des organisations et des organismes de sÃ©curitÃ© ne pourra que renforcer cette cyber armÃ©e que la Commission EuropÃ©enne est en train de mettre en place.

De plus, le fait que lâ□□ENISA prodigue des recommandations est en effet indispensable mais il ne faut surtout pas que les entreprises restent passives pour autant et attendent de recevoir ces conseils, elles doivent Ãªtre soumises Ã des politiques de sÃ©curitÃ© strictes qui seront bien plus efficaces au final. En cybersÃ©curitÃ©, lâ□□union fait la cyber force et il est donc plus que jamais essentiel de lutter ensemble contre les nouvelles attaques et prÃ©venir toute intrusion dans les systÃ¨mes. Â»