SÃ©curitÃ© : CybercriminalitÃ©, l'OTAN n'est pas Ã©pargnÃ©.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 10/6/2013 11:30:00

L'OTAN a admis avoir subi plus de 2 500 tentatives dâattaques informatiques en 2012. Bien qu'aucune nâait rÃ©ussi Ã contourner le systÃ¨me de sÃ©curitÃ© de l'OTAN, une dizaine d'attaques par mois ont Ã©tÃ© jugÃ©es sÃ©rieusement compromettantes pour ses rÃ©seaux.

L'annonce a Ã©tÃ© faite suite Ã une rÃ©union dâexperts de la DÃ©fense Ã Bruxelles, dans le but dâÃ©changer sur la mise en place dâune cellule d'experts Â« Ã©quipes de rÃ©action rapide Â» afin dâaider les membres de l'OTAN Ã dÃ©fendre leurs rÃ©seaux contre les attaques. De la mÃªme maniÃ¨re, BSkyB, chaine de tÃ©lÃ©vision britannique, a Ã©galement rÃ©vÃ©lÃ© cette semaine avoir commencÃ© Ã Ã©changer des renseignements avec ses concurrents dans un effort commun de lutte contre la cybercriminalitÃ©.

Jean-Pierre Carlin, Directeur rÃ©gional pour lâEurope du Sud chez LogRhythm, commente :

Â« *Pour une organisation comme l'OTAN, les consÃ©quences d'une cyberattaque rÃ©ussie pourraient Ãªtre extrÃªmement dommageables et causer la perte dâinformations trÃ¨s sensibles, voire de vies humaines. Les cybercriminels mettent en place des attaques de plus en plus sophistiquÃ©es et, bien qu'ils aient Ã©chouÃ© dans leur tentative de violation des rÃ©seaux de l'OTAN Ã ce jour, cela ne signifie pas quâils nây parviendront pas Ã lâavenir.*

On dit que le vrai pouvoir est la connaissance et cela est particuliÃ¨rement pertinent lorsquâil s'agit de toujours garder une longueur d'avance pour se dÃ©fendre contre les cybercriminels. Il est donc encourageant de constater que des organisations telles que l'OTAN augmentent la quantitÃ© d'informations qu'ils partagent en interne. Cependant, beaucoup pourraient Ã©galement suivre lâexemple de BSkyB et partager leurs connaissances en externe afin d'Ã©largir les forces

communes. Alors que plusieurs entreprises peuvent penser que la divulgation de ces informations Ã des concurrents est un risque, il reste toujours moindre quâ□□une cyber-attaque rÃ©ussie.

Afin de s'armer dâ□□autant de connaissances que possible, les entreprises doivent constamment surveiller leurs rÃ©seaux afin dâ□□Ã©tablir une activitÃ© normale de rÃ©fÃ©rence. DÃ¨s lors, toute anomalie sur le rÃ©seau peut Ãªtre identifiÃ©e en temps rÃ©el. Avec un tel niveau de traÃ§abilitÃ©, les stratÃ©gies de rÃ©duction des dommages peuvent Ãªtre lancÃ©es, et les cyber-menaces maÃ®trisÃ©es. Une fois que tout le monde sera armÃ© du mÃªme niveau d'information, le partage de renseignement deviendra une stratÃ©gie encore plus efficace. Â»