EmployÃ©, complice des cybercriminels Ã son insu ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 11/1/2019 13:00:00

Selon une Ã©tude rÃ©cente, la moitiÃ© des PME franÃ§aises admettent ne pas former leurs salariÃ©s Ã la cybersÃ©curitÃ©. Or, il est dÃ©sormais certain que toute entreprise sera un jour confrontÃ©e Ã une attaque, quelle que soit sa taille ou son industrie, et les employÃ©s constituent une rÃ©elle vulnÃ©rabilitÃ©.

Ces derniers peuvent bien sÃ»r Ãªtre piÃ©gÃ©s et devenir une menace interne Ã leur insu, en dÃ©voilant leurs identifiants Ã un hacker suite Ã une attaque de phishing, par exemple.

Toutefois, il est aussi possible quâ□□ils tentent de compromettre des donnÃ©es de leur plein grÃ©, notamment Ã cause dâ□□un diffÃ©rend, un renvoi ou encore Ã des fins vÃ©nales.

Pierre-Louis Lussan, Country Manager France, chez Netwrix, estime que le risque de la menace interne ne doit pas Ãªtre pris Ã la lÃ©gÃ¨re, ou ignorÃ©.Â

Câ□□est pourquoi les entreprises doivent impÃ©rativement Ãªtre en mesure de surveiller les activitÃ©s sur leur rÃ©seau, et Ãªtre alertÃ©es dÃ¨s quâ□□une situation inhabituelle se produit :

Â« Au quotidien, le comportement des employÃ©s sur le serveur est rÃ©pÃ©titif : ils accÃ¨dent aux mÃªmes systÃ¨mes et informations, pendant les mÃªmes horaires, et toujours de la mÃªme maniÃ¨re.Â

Cette routine reprÃ©sente finalement une aide cruciale pour les organisations, qui peuvent dÃ©finir un comportement type et dÃ©terminer ainsi une dÃ©rive, signe dâ□□une tentative de compromission.

En effet, il leur suffit de dÃ©ployer des outils qui surveillent automatiquement les opÃ©rations menÃ©es par les utilisateurs, et de configurer des alertes automatiques en cas de violations des rÃ¨gles de sÃ©curitÃ© ou de comportements suspects.Â

En outre, elles doivent Ãªtre Ã l'affÃ»t de tout pic d'activitÃ© autour des actifs critiques, leur protection Ã©tant une prioritÃ©.

Lorsque l'Ã©quipe informatique reÃ§oit une alerte Ã propos d'une anomalie â par exemple, si une personne modifie au moins dix fichiers en moins de 600 secondes â il est nÃ©cessaire d'enquÃªter rapidement sur lâincident, pour intervenir avant que des dommages ne soient effectifs.

Il faut Ã©galement dÃ©terminer si les informations modifiÃ©es sont sensibles, pour prioriser les enquÃªtes et interventions. Ainsi, si un collaborateur dÃ©cide de vendre des donnÃ©es Ã un concurrent, devenant alors une menace interne, lâÃ©quipe IT peut rapidement repÃ©rer son transfert sur une clÃ© USB dâun grand nombre dâinformations Ã partir d'un fichier sensible.

En recevant Ã temps lâalerte, cet utilisateur malveillant peut Ãªtre stoppÃ©, et lâentreprise conserve sa compÃ©titivitÃ© et prÃ©serve son image de marque.

Il ne faut pas oublier que la plupart des menaces internes ne sont pas malveillantes, mais rÃ©sultent dâerreurs humaines qui ne peuvent Ãªtre Ã©vitÃ©es que via une sensibilisation constante des Ã©quipes Ã la cybersÃ©curitÃ© et la mise en place dâoutils adaptÃ©s aux besoins spÃ©cifiques de lâorganisation.

Le vÃ©ritable problÃ¨me rÃ©side dans la compromission potentielle de tout compte utilisateur par des cybercriminels. Ces derniers usent de techniques dâattaque toujours plus sophistiquÃ©es et abusent trop souvent de la naÃ¯vetÃ© des utilisateurs, ou de leur mÃ©connaissance sur les cyber-risques.

Par consÃ©quent, face Ã la menace interne, les organisations doivent faire leur maximum pour Ã©viter les erreurs opÃ©rationnelles, en Ã©clairant rÃ©guliÃ¨rement les utilisateurs sur les bonnes pratiques de sÃ©curitÃ© Ã adopter.Â

En outre, la combinaison dâune visibilitÃ© complÃ¨te sur les opÃ©rations menÃ©es dans le rÃ©seau Ã des alertes automatiques signalant toute activitÃ© vraisemblablement suspecte, permettra aux Ã©quipes informatiques dâagir rapidement et de contrer Ã temps les tentatives de compromission.

Une sÃ©curitÃ© efficace repose donc sur une collaboration continue entre tous les membres dâune entreprise, et sur une organisation rationnelle et structurÃ©e, facilitant ainsi lâidentification de comportements rÃ©seau dÃ©viants. Â»

Pierre-Louis Lussan, Country Manager France, chez Netwrix