Telindus renforce sa lutte contre les cyber-attaques
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 28/11/2014 13:00:00

En 2014, 42,8 millions de cyber-attaques ont eu lieu, et ce, pour un coÃ»t annuel de 2,7 millions de dollars . Chaque jour, des attaques toujours plus complexes et furtives endommagent les rÃ©seaux informatiques et mettent en risque la valeur des entreprises.

Dans ce contexte de menaces permanentes, Telindus dÃ©ploie ses forces pour sÃ©curiser les donnÃ©es sensibles des entreprises. Le Security Operation Center (SOC) permet de construire des schÃ©mas de dÃ©fense efficaces, de surveiller le SystÃ¨me dâ□□Information, de dÃ©tecter, dâ□□analyser les attaques pour alerter et remÃ©dier. Le Soc de Telindus construit des stratÃ©gies de dÃ©fense propre Ã chaque contexte mÃ©tier toujours en phase avec la politique de sÃ©curitÃ© de ses clients

Le Centre de SÃ©curitÃ© OpÃ©rationnel (SOC) de Telindus est un centre de services dÃ©diÃ© Ã l'exploitation des dispositifs de sÃ©curitÃ© de lâ□□entreprise. La rÃ©ussite de la mission du SOC dÃ©pend de la bonne conjugaison de 3 facteurs : une plateforme dâ□□outils qui permet dâ□□optimiser la dÃ©tection et la gestion des nouvelles attaques, lâ□□organisation humaine composÃ©e dâ□□ingÃ©nieurs et dâ□□experts de sÃ©curitÃ© certifiÃ©s et enfin des processus dâ□□application adaptÃ©s Ã chaque contexte business.

A travers la dÃ©lÃ©gation partielle ou totale des services dâ□□un SOC, les entreprises tÃ©moignent de la nÃ©cessitÃ© dâ□□obtenir une meilleure visibilitÃ© sur leurs infrastructures mais surtout de protÃ©ger leurs intÃ©rÃªts vitaux grÃ¢ce Ã une organisation efficace capable dâ□□agir trÃ¨s vite et de sâ□□engager en cas dâ□□attaques avÃ©rÃ©e.

La mission de Telindus

Le SOC Telindus exerce plusieurs missions afin de dÃ©fendre, de surveiller, dÃ©tecter et analyser les attaques auxquelles doivent faire face les SystÃ¨mes dâ□□Informations

- DÃ©finir le pÃ©rimÃ¨tre Ã protÃ©ger et les rÃ¨gles de sÃ©curitÃ© adaptÃ© aux enjeux mÃ©tiers : lâ□□ingÃ©nieur expert sÃ©curitÃ© se doit de dÃ©finir avec le responsable des opÃ©rations de sÃ©curitÃ© des procÃ©dures personnalisÃ©es bloquant les attaques.

- DÃ©tecter et Ã©valuer les attaques pour recommander les solutions. AprÃ¨s une alerte, lâ□□ingÃ©nieur examine les Ã©vÃ©nements malveillants pour dÃ©finir sa sÃ©vÃ©ritÃ© et recueillir les informations pertinentes lui permettant de lutter contre celle-ci. Il peut alors anticiper de futures intrusions. Chaque mois, les incidents sont analysÃ©s et rapprochÃ©s les uns des autres pour obtenir une analyse contextuelle plus riche, afin de dÃ©finir le danger que court le client, les consÃ©quences liÃ©es aux attaques et les Ã©ventuelles mesures Ã prendre.

- Renforcer la sÃ©curitÃ© en assurant une meilleure visibilitÃ© de lâ□□activitÃ© du SI. Le SOC sâ□□appuie sur des outils capables de corrÃ©ler les Ã©vÃ©nements de sÃ©curitÃ© et ainsi dâ□□affiner la rÃ©ponse pour bloquer les attaques de faÃ§on optimale. En effet, quand les Ã©vÃ©nements sont analysÃ©s sÃ©parÃ©ment, ils ne dÃ©clenchent pas toujours une alerte. Pourtant lorsquâ□□ils sont associÃ©s, ils peuvent Ãªtre la trace dâ□□une tentative dâ□□intrusion. De plus, ces outils Ã©vitent de dÃ©clencher une alerte lorsque la cible nâ□□est pas vulnÃ©rable Ã une attaque.

Les avantages dâ□□un service sur-mesure

Tout type dâ□□entreprise a besoin dâ□□un SOC dÃ¨s lors que celle-ci a des donnÃ©es informatiques Ã traiter. Pour que celui-ci puisse Ãªtre activÃ©, il faut Ãªtre en mesure de collecter les donnÃ©es en un point unique. Telindus sâ□□adapte alors Ã la stratÃ©gie de sÃ©curitÃ© du client en mettant en place soit une solution in situ, dans les locaux du client, soit en lâ□□externalisant, dans le Datacenter de Telindus.

En sâ□□appuyant sur un data center et une organisation certifiÃ©e ISO 27001, Telindus fournit un service de surveillance, de dÃ©tection et de rÃ©action avec le niveau dâ□□exigence adaptÃ© Ã chaque client et contexte.
Par cette approche, Telindus rend le service "SOC" accessible Ã toutes les entreprises.

Â« *Aujourdâ□□hui, alors que lâ□□informatique est prÃ©sente dans tous les secteurs et Ã toutes les Ã©chelles il est vital de mettre en place des solutions de cyberdÃ©fense stables et pÃ©rennes. Surveiller, dÃ©tecter et rÃ©agir, voici notre approche de la cyberdÃ©fense. Surveiller toutes les couches du systÃ¨me dâ□□information.*

DÃ©tecter tous les incidents de sÃ©curitÃ©, quâ□□ils soient liÃ©s Ã un problÃ¨me technique, humain ou environnemental. RÃ©agir face Ã un incident en prenant en compte toutes les informations liÃ©es Ã lâ□□Ã©vÃ©nement et en y remÃ©diant en sâ□□appuyant sur une procÃ©dure liant le traitement technique et organisationnel de lâ□□incident,Â» explique Noel Chazotte, Consultant Marketing SÃ©curitÃ© chez ***Telindus***