Repenser sa politique sÃ©curitÃ© : un point-clÃ© pour les entreprises
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 28/11/2017 13:00:00

La sÃ©curisation du systÃ¨me dâ□□information se positionne comme un axe de vigilance stratÃ©gique pour lâ□□ensemble des entreprises. En effet, de plus en plus exposÃ©es Ã des attaques de diffÃ©rentes natures (notamment le vol de donnÃ©es stratÃ©giques), les entreprises doivent repenser en profondeur leur gouvernance en matiÃ¨re de cyber sÃ©curitÃ© afin de ne pas voir leur SI infectÃ©.

Aujourdâ□□hui, la trÃ¨s grande majoritÃ© des attaques est dirigÃ©e directement vers lâ□□utilisateur. Les scÃ©narii les plus courants dâ□□infection sont : des piÃ¨ces jointes malveillantes dans un mail, des sites Web infectÃ©s, des publicitÃ©s malveillantes, des URL malveillantes et le piratage psychologique.

Nul nâ□□est Ã lâ□□abri, comme le prouvent les derniÃ¨res attaques spectaculaires qui ont paralysÃ© de nombreuses grandes entreprises dans lâ□□ensemble des secteurs dâ□□activitÃ©.

DÃ©finir une rÃ©elle stratÃ©gie de dÃ©fense au niveau utilisateur

Dans ce contexte, une approche Ã©tendue pour renforcer la sÃ©curitÃ© des endpoints (pÃ©riphÃ©riques utilisateurs) est nÃ©cessaire.

En effet, sâ□□appuyer sur un simple antivirus nâ□□est plus adaptÃ©.

Bien sÃ»r, il serait naÃ¯f de penser quâ□□il existe une solution miracle pour protÃ©ger son organisation contre tous les types de menaces existantes.Â

Pour autant, la sÃ©curitÃ© des infrastructures peut Ãªtre radicalement renforcÃ©e grÃ¢ce Ã une approche de protection multi-niveaux.

A ce titre, une stratÃ©gie prenant en compte diffÃ©rents facteurs complÃ©mentaires semble adaptÃ©e et rÃ©pondre assez efficacement aux attentes des entreprises souhaitant bÃ©nÃ©ficier dâ□□un haut niveau de sÃ©curitÃ© informatique.

Cette derniÃ¨re vise principalement Ã prendre en compte toutes les actions nÃ©cessaires afin de sÃ©curiser tous les types de endpoint : ordinateur fixe ou mobile, tablette et smartphone.

Parmi les diffÃ©rents dispositifs Ã mettre en place, nous pouvons notamment Ã©voquer cinq grandes actions complÃ©mentaires :

La dÃ©couverte et lâ□□inventaire : travail prÃ©liminaire indispensable, il sâ□□agit de parfaitement connaÃ®tre son parc afin de protÃ©ger lâ□□ensemble des pÃ©riphÃ©riques utilisÃ©s par les collaborateurs. Ce point est notamment stratÃ©gique avec le dÃ©veloppement de la mobilitÃ© et lâ□□utilisation de terminaux mobiles personnels dans le cadre professionnel.

La gestion des correctifs de sÃ©curitÃ© : la premiÃ¨re ligne de dÃ©fense consiste Ã dÃ©ployer le plus rapidement possible les correctifs systÃ¨mes et applicatifs sur lâ□□ensemble du parc afin de ne pas sâ□□exposer Ã des menaces pouvant se rÃ©pandre via des failles de sÃ©curitÃ© identifiÃ©es et publiques.

Le contrÃ´le des applications : il est fondamental dâ□□avoir une vigilance extrÃªme sur ce point et dâ□□Ã©tablir une stratÃ©gie flexible permettant Ã la fois dâ□□accepter uniquement lâ□□exÃ©cution dâ□□applications autorisÃ©es par le service informatique, sans pour autant perturber la productivitÃ© des utilisateurs.

La gestion des privilÃ¨ges : Lâ□□attribution des privilÃ¨ges administrateur pour un utilisateur est un facteur de risque important dans le processus dâ□□infection par un malware. Il est donc ici question de restreindre le niveau de privilÃ¨ge des utilisateurs tout en autorisant une Ã©lÃ©vation de leurs droits pour certaines actions identifiÃ©es afin que ces derniers restent pleinement productifs.

Piloter efficacement sa conformitÃ© : enfin, il est indispensable de bÃ©nÃ©ficier dâ□□indicateurs et dâ□□informations dÃ©taillÃ©es sur les diffÃ©rents niveaux de sÃ©curitÃ© appliquÃ©s afin de mesurer les Ã©carts de configuration et de pouvoir planifier les actions correctrices adÃ©quates.

La rÃ©ponse aux diverses menaces passe donc aujourdâ□□hui par une amÃ©lioration de la protection de lâ□□Ã©cosystÃ¨me digital des entreprises (rÃ©seau, datacenter, endpoint).

Au niveau de lâ□□utilisateur, lâ□□objectif principal est de rÃ©duire les points de vulnÃ©rabilitÃ© et minimiser les vecteurs dâ□□attaques en mettant en Å□uvre une stratÃ©gie de dÃ©fense complÃ¨te (dÃ©couverte et inventaire, antivirus, correctifs, contrÃ´le des applications, gestion des privilÃ¨ges) qui amÃ©liore drastiquement la protection contre les cyberattaques.

Â Laurent Ostrowski â□□ Consultant, Cegedim Outsourcing