

Repenser sa politique s curit  : un point-cl  pour les entreprises

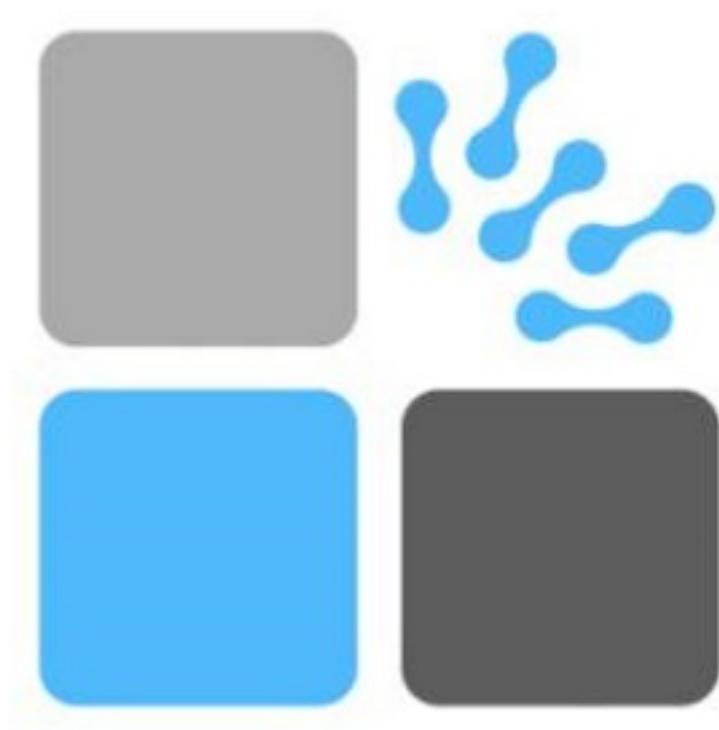
S curit 

Post  par : JulieM

Publi e le : 28/11/2017 13:00:00

La s curisation du syst me d'information se positionne comme un axe de vigilance strat gique pour l'ensemble des entreprises. En effet, de plus en plus expos es   des attaques de diff rentes natures (notamment le vol de donn es strat giques), les entreprises doivent repenser en profondeur leur gouvernance en mati re de cyber s curit  afin de ne pas voir leur SI infect .

Aujourd'hui, la tr s grande majorit  des attaques est dirig e directement vers l'utilisateur. Les sc narii les plus courants d'infection sont : des pi ces jointes malveillantes dans un mail, des sites Web infect s, des publicit s malveillantes, des URL malveillantes et le piratage psychologique.



Nul n'est   l'abri, comme le prouvent les derni res attaques spectaculaires qui ont paralys  de nombreuses grandes entreprises dans l'ensemble des secteurs d'activit .

D finir une r elle strat gie de d fense au niveau utilisateur

Dans ce contexte, une approche  tendue pour renforcer la s curit  des endpoints (p riph riques utilisateurs) est n cessaire.

En effet, s'appuyer sur un simple antivirus n'est plus adapt .

Bien s r, il serait n f de penser qu'il existe une solution miracle pour prot ger son organisation contre tous les types de menaces existantes. 

Pour autant, la sécurité des infrastructures peut être radicalement renforcée grâce à une approche de protection multi-niveaux.

A ce titre, une stratégie prenant en compte différents facteurs complémentaires semble adaptée et répondre assez efficacement aux attentes des entreprises souhaitant bénéficier d'un haut niveau de sécurité informatique.

Cette dernière vise principalement à prendre en compte toutes les actions nécessaires afin de sécuriser tous les types de endpoint : ordinateur fixe ou mobile, tablette et smartphone.

Parmi les différents dispositifs à mettre en place, nous pouvons notamment évoquer cinq grandes actions complémentaires :

La découverte et l'inventaire : travail préliminaire indispensable, il s'agit de parfaitement connaître son parc afin de protéger l'ensemble des périphériques utilisés par les collaborateurs. Ce point est notamment stratégique avec le développement de la mobilité et l'utilisation de terminaux mobiles personnels dans le cadre professionnel.

La gestion des correctifs de sécurité : la première ligne de défense consiste à déployer le plus rapidement possible les correctifs systèmes et applicatifs sur l'ensemble du parc afin de ne pas s'exposer à des menaces pouvant se répandre via des failles de sécurité identifiées et publiques.

Le contrôle des applications : il est fondamental d'avoir une vigilance extrême sur ce point et d'établir une stratégie flexible permettant à la fois d'accepter uniquement l'exécution d'applications autorisées par le service informatique, sans pour autant perturber la productivité des utilisateurs.

La gestion des privilèges : L'attribution des privilèges administrateur pour un utilisateur est un facteur de risque important dans le processus d'infection par un malware. Il est donc ici question de restreindre le niveau de privilège des utilisateurs tout en autorisant une élévation de leurs droits pour certaines actions identifiées afin que ces derniers restent pleinement productifs.

Piloter efficacement sa conformité : enfin, il est indispensable de bénéficier d'indicateurs et d'informations détaillées sur les différents niveaux de sécurité appliqués afin de mesurer les écarts de configuration et de pouvoir planifier les actions correctrices adéquates.

La réponse aux diverses menaces passe donc aujourd'hui par une amélioration de la protection de l'écosystème digital des entreprises (réseau, datacenter, endpoint).

Au niveau de l'utilisateur, l'objectif principal est de réduire les points de vulnérabilité et minimiser les vecteurs d'attaques en mettant en œuvre une stratégie de défense complète (découverte et inventaire, antivirus, correctifs, contrôle des applications, gestion des privilèges) qui améliore drastiquement la protection contre les cyberattaques.

À Laurent Ostrowski @ Consultant, Cegedim Outsourcing