Sécuriser les réseaux d'entreprise : Microsoft partage ses méthodes

Plutôt que de livrer un énième plaidoyer sur les cyber menaces qui pèsent sur les entreprises pour mieux mettre en avant ses solutions, Microsoft explique comment sa propre équipe en charge de la sécurité informatique protège son réseau en appliquant quelques règles de base.

Au cœur du réacteur, les personnes ayant un accès administrateur dont il faut protéger et contrôler les interventions. "Pour améliorer la protection de notre organisation, il est important de limiter le nombre de personnes qui ont un accès privilégié et de mettre en place des contrôles élevés pour savoir quand, comment et où les comptes administrateurs peuvent être utilisés", explique Microsoft.

Les accès à privilèges sous contrôle

La première des recommandations élémentaires est que ces administrateurs utilisent un terminal uniquement dédié aux tâches d'administration du réseau qui doit être parfaitement à jour.

"Réglez les contrôles de sécurité à des niveaux élevés et empêchez les tâches administratives d'être exécutées à distance", conseille l'éditeur qui précise que ses administrateurs doivent utiliser une carte électronique pour accéder à ce compte.

Il est aussi conseillé de créer un compte administrateur dans un espace de noms d'utilisateur/forêt séparé qui ne peut pas accéder à Internet et qui doit être différent de l'identité professionnelle normale de l'employé.

Troisième règle appliquée chez Microsoft : n'attribuer aucun droit par défaut aux comptes administrateurs et exiger que ces derniers demandent des privilèges juste à temps qui leur donnent accès pour une durée limitée et les enregistrent dans un système.

"Les allocations budgétaires peuvent limiter le montant que vous pouvez investir dans ces trois domaines ; cependant, nous vous recommandons quand même de faire les trois au niveau qui convient à votre organisation. Étalonnez le niveau des contrôles de sécurité de l'appareil sécurisé en fonction de votre profil de risque", recommande Microsoft.

A lire : Sécuriser les accès et les identités : 4 questions pour maitriser l'IAM