Google dévoile un peu la sécurité de ses datacenters

Dans cette période où la sécurité informatique est omniprésente dans l'actualité, Google a profité de sa conférence NEXT pour lever un peu le voile sur les mesures prises pour protéger physiquement ses datacenters contre les intrusions. Cœur stratégique des services de Mountain View, les datacenters ne sont accessibles qu'à moins de 1% des 60 000 salariés de la firme. Un moyen déjà de filtrer les accréditations pour rentrer dans les saints des saints.

Gardiennage, biométrie et laser

Pour y rentrer, il faudra montrer patte blanche, prévient Joe Kava, vice-président des opérations des datacenters, dans un blog. Les immeubles sont régulièrement surveillés par des gardes entraînés et formés à la protection de ce type d'infrastructure. Ils assurent la sécurité à l'extérieur des bâtiments comme les points d'entrée des véhicules, mais aussi dans les immeubles en accompagnant physiquement les personnes. En complément, une surveillance vidéo est assurée 24/24 et 7/7.

Avant d'entrer dans le datacenter, la personne devra se soumettre à plusieurs contrôles. Il doit par exemple disposer d'un badge d'accès nominatif comprenant son profil et ses autorisations pour travailler sur telle ou telle partie du datacenter. Ce badge est sécurisé pour éviter les contrefaçons. En plus de cette authentification, un contrôle biométrique est réalisé dans un sas, comme on peut le constater dans une vidéo sur YouTube, titrée 360 degree data center tour. Ce contrôle peut être soit oculaire (reconnaissance de l'iris) ou digitale (via les empreintes).

Si quand bien même, un intrus ingénieux arrivait dans les salles du datacenter, il devrait se méfier du sol. Ce dernier est truffé de détection d'intrusion par faisceaux laser capable de se déclencher aux moindres mouvements. Il faudrait donc l'habileté d'une star de cinéma pour se mouvoir dans ce labyrinthe de laser pour ne pas faire retentir les alarmes (comme Vincent Cassel, interprète du baron François Toulour dans *Oceans Twelve*).

Du cousu main pour contrôler la sécurité

Et s'il y arrivait, il se heurterait à la politique très stricte de Google en matière de stockage par exemple. « *Nous avons un cycle de vie très réglementé pour le stockage, il suit le disque dur dès qu'il intègre pour la première fois une machine jusqu'au contrôle de son effacement et de sa destruction* », explique Joe Kava. Et d'ajouter, « *la sécurité de l'information et la sécurité physique vont main dans la main* ». Pour lui un des atouts pour réussir cela est de gérer ses propres datacenters et de faire beaucoup de choses par soi-même, ce qui limite les expositions aux failles.

Ainsi, les serveurs utilisés par Google ne comprennent pas de fonctionnalités inutiles ou de composants non essentiels comme des connecteurs pour périphérique, des cartes vidéo ou des chipsets. De même, tous les serveurs de production fonctionnent sur une version sécurisée de

Linux et les ressources sont prises en charge dynamiquement avec un minimum d'implications humaines. Face à la complexité des processus d'interconnexion, de déploiement, Google utilise à la fois le machine learning et le software defined pour automatiser ces différentes tâches. Il faut dire que les datacenters de Google sont hors-normes. Dans la vidéo citée précédemment, on apprend qu'ils peuvent accueillir 75 000 machines par bâtiment et avoir une bande passante de 1 Petabit/seconde à travers une technologie réseau baptisée Jupiter. De même, les datacenters du monde entier sont reliés entre eux par un backbone nommé B4. Et la firme a de grandes ambitions dans le Cloud et a confirmé à la conférence NEXT sa volonté d'ouvrir 12 datacenters de plus dans un proche avenir.

A lire aussi :

Cloud : comment Google tente de refaire son retard

Google veut réformer les disques durs pour datacenters