Puce de sécurité, KVM renforcé : les recettes sécurité de l'infra de Google

Google a publié un document sur la sécurité de son infrastructure de son propre Cloud et des services de Cloud public qu'il propose. Dans ce document, la filiale d'Alphabet souligne avoir 6 niveaux de sécurité (cf ci-dessous) allant de la sécurité opérationnelle en passant par la communication Internet, le déploiement de services à l'infrastructure hardware.

Une puce de sécurité pour les serveurs

Et c'est sur dernier point que le document de Google nous livre des éléments intéressants. En effet, la firme explique que ses datacenters comprennent des milliers de serveurs connectés au réseau local. Google construit ses propres serveurs à partir de composants choisis et audités auprès de différents fournisseurs. Mais la société « *conçoit également des puces personnalisées, y compris une puce dédiée à la sécurité du hardware. Elle est actuellement déployée sur les serveurs et des périphériques. Ces puces nous permettent d'identifier et d'authentifier en toute sécurité les terminaux Google au niveau hardware* ».

La firme de Mountain View ne donne pas plus de précision sur cette puce dédiée à la sécurité. On sait qu'elles travaillent en parallèle d'autres solutions de sécurité comme les signatures cryptographiques. Celles-ci sont utilisées sur des éléments de bas niveau comme le BIOS, le bootloader, le noyau et l'image de l'OS. « *Ces signatures peuvent être validées à chaque démarrage ou mise à jour* », explique le document. Et d'ajouter que « *à chaque nouvelle génération d'équipements, nous nous efforçons d'améliorer continuellement la sécurité. Par exemple en fonction du design des serveurs, nous renforçons la chaîne du boot soit via un micro-contrôleur exécutant du code de sécurité écrit par Google ou via la puce de sécurité conçue par Google citée précédemment* ».

Processus pour l'élimination des disques durs et SSD

Ces indications s'inscrivent dans la suite d'une présentation lors de la conférence NEXT en mars dernier. Joe Kava, vice-président des opérations des datacenters avait levé le voile sur quelques éléments de la sécurité des datacenters de la firme. Sur la partie hardware, on apprenait que 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.

Toujours dans ce document, on retrouve des éléments sur la sécurité du stockage des données. « *Nous activons le support le chiffrement matériel du disque dur et des SSD, et surveillons méticuleusement chaque disque tout au long de son cycle de vie. Quand ils sont déclassés, ils sont nettoyés en utilisant un processus à plusieurs étapes dont deux vérifications indépendantes. Une fois ce process réalisé, les disques*

sont physiquement détruits sur site. »

Code source protégé et KVM revisité

On en sait plus aussi sur le code source de Google. *« Il est stocké dans un référentiel central où les versions passées et actuelles des services sont auditables. L'infrastructure peut être configurée pour que les binaires d'un service soient élaborés à partir du code source analysé, validé et testé. »* Le document ajoute que *« les examens de code nécessitent l'inspection et l'approbation d'au moins un ingénieur autre que l'auteur et le système veille à ce que les modifications de code soient approuvées par le détenteur de ce système »*. L'objectif est d'éviter l'intégration d'un code malveillant dans le système par quelqu'un d'interne ou un pirate extérieur.

Enfin terminons sur le Cloud où on apprend que le IaaS de Google a quelques particularités. Il y a plusieurs niveaux de sécurité dans Compute Engine explique la firme allant du SSL/TLS à la double identité VM et gestionnaire de VM. Mais le moins connu est que l'isolation des machines virtuelles est assurée par une virtualisation matérielle reposant sur une version personnalisée de KVM. « *Nous avons étoffé notre implémentation particulière de KVM en déplaçant des éléments de contrôle et d'émulation matérielle dans un processus en dehors du Kernel.* » Et d'ajouter : « *Nous avons également testé de manière approfondie le noyau du KVM en utilisant des techniques comme le fuzzing, l'analyse statique et l'examen manuel du code.* » Google en profite pour souligner qu'il est le plus gros contributeur de CVE et de fixation d'erreur sur l'hyperviseur Open Source.

Au final, Google livre un document touffu sur sa sécurité. Un moyen de rassurer les clients et les futurs clients de son offre Cloud. Un message aussi à l'attention des pirates pour montrer que le niveau de sécurité est très élevé.

A lire aussi :

Google a blindé la sécurité d'Android 7.0 Nougat

Sécurité : Google finalise sa mue en HSTS