GitLab : « Le modèle Zero Trust de sécurité est notre crédo »

Les entreprises sont toujours plus nombreuses à opter pour une approche **Zero Trust** (« zéro confiance ») de la sécurité cyber. Elles le font en priorité pour réduire l'accès inconsidéré de collaborateurs aux plateformes et aux applications métiers de l'entité concernée.

GitLab, gestionnaire de dépôt de code source orienté DevOps, fait partie des organisations qui ont intégré ce modèle Zero Trust et se détournent d'approches traditionnelles.

Mark Loveless*, ingénieur sécurité chez GitLab, fait le point d'une approche qui permet à l'entreprise américaine de renforcer le contrôle de ses systèmes et des données qu'ils contiennent, sans sacrifier la confiance de ses (télé)travailleurs et utilisateurs dans le monde.

Silicon.fr : L'industrie numérique demande aux utilisateurs et aux clients de lui accorder leur confiance, tout en faisant la promotion du modèle de sécurité Zero Trust (« zéro confiance »). Qu'en pense GitLab ?

Mark Loveless : En tant que société, GitLab applique actuellement les principes fondamentaux du Zero Trust dans son programme global de sécurité. Cette approche garantit la protection des actifs de GitLab lorsque ses équipes y ont accès. Vérifier qu'un employé est bien celui qu'il prétend être lorsqu'il se connecte à l'une des plateformes de la société fait partie de ces principes fondamentaux. Nous les appliquons par le biais d'un identifiant utilisateur avec authentification à deux facteurs. Par ailleurs, nous nous efforçons de garantir que ceci fonctionne de deux manières : d'une part, nous savons que l'employé est celui qu'il prétend être et, d'autre part, nous voulons être sûrs que le collaborateur sait qu'il se connecte à une plateforme GitLab et non à un site faux ou frauduleux.

Pour tout dire, GitLab estime que le concept de « vérifier avant de faire confiance », systématique dans le modèle Zero Trust, est une bonne chose. J'ajoute que notre entreprise est extrêmement transparente. Nous publions plus largement nos mécanismes et nos systèmes internes que ne le fait la majorité des entreprises. Et nous engageons un débat ouvert avec le public. Certains de mes amis qui travaillent dans d'autres sociétés me disent qu'autant de transparence serait un cauchemar à gérer pour leur société en termes de relations publiques. Nous pensons au contraire que l'idée de transparence et d'ouverture permet à notre entreprise d'aller de l'avant. À notre avis, ce parti pris est avantageux pour toute organisation, pas seulement GitLab. Ainsi, nous pensons que les clients peuvent nous faire confiance et éprouver cette confiance en voyant exactement ce que nous faisons.

Selon vous, quel est le lien entre la cybersécurité Zero Trust et le modèle Security by Design ?

M.L. : La sécurité réseau d'une part, la sécurité produit/projet d'autre part. Ainsi, les principes de Security by Design (sécurité dès la conception, en français) impliquent l'intégration de la sécurité dans la structure globale d'une organisation. Chez GitLab, cette intégration se fait dans nos produits et dans les processus de création de ces produits.

Quant au Zero Trust, il concerne davantage la sécurité du réseau de l'entreprise. Il y a quelques années, une entreprise installait tous ses employés dans un bâtiment, avec les ordinateurs de l'organisation et un contrôle strict du périmètre. La sécurité informatique était liée à un lieu physique. Dans les organisations d'aujourd'hui, les collaborateurs travaillent à distance, depuis une multitude de lieux différents. Les actifs des sociétés sont déplacés vers le cloud et l'architecture de sécurité de l'information est moins centrée sur le lieu physique.

Chez GitLab, ce phénomène est poussé à l'extrême : nous travaillons tous à distance et nous sommes tous basés sur le cloud. C'est ici que l'approche Zero Trust prend tout son sens : il est impossible de faire confiance au réseau lorsque les employés se connectent. Nous devons contrôler/autoriser l'accès aux actifs de la société, quel que soit l'emplacement physique des employés. Je répète, Zero Trust est une approche qui permet de vérifier que la personne est exactement celle qu'elle dit être. Cet accès est restreint, dès l'ouverture de session, de telle façon qu'un employé a accès à tels documents et uniquement à ces documents.

Avec la progression des principes Zero Trust, nous ajouterons l'identification de l'ordinateur portable de l'utilisateur (et de la configuration de sécurité de son terminal) au moment de l'authentification. Nous étendrons même ce contrôle aux programmes internes et aux processus automatisés pour affiner le contrôle de notre environnement. Le contrôle de nos systèmes et des données qu'ils contiennent sera ainsi renforcé. Quant aux principes de base de Security by Design, ils sont difficiles à mettre en œuvre dans leur intégralité, pour la plupart des entreprises, du fait de la suppression du périmètre et du passage à une architecture cloud. Chez GitLab, le Zero Trust nous fournit un moyen d'utiliser le modèle de Security by Design dans l'environnement cloud et sans périmètre dans lequel nous évoluons.

La collecte de données que pratique GitLab – voir l'épisode du service de télémétrie sans opt-out – n'a pas toujours été bien reçue par les développeurs. Où en sommes-nous aujourd'hui ?

M.L. : Nous nous efforçons toujours de maintenir l'équilibre, mais en veillant à impliquer nos clients et la communauté des développeurs. Initialement, la télémétrie était conçue pour l'amélioration des produits : les nouvelles fonctionnalités sont-elles utilisées ? Les anciennes sont-elles obsolètes ? Cependant, pour que ceci soit bien réalisé, il faut assurer la transparence. C'est ce que nous essayons de faire. La plupart des organisations résolvent leurs faux pas à huis clos. Chez GitLab, nous le faisons ouvertement.

Vis-à-vis de nos clients et de la communauté des développeurs, nous avons la responsabilité d'agir dans l'intérêt de chacun. Ceci est la clé du succès de GitLab. De plus, nous estimons qu'en agissant ainsi nous donnons un exemple de « bonne pratique ». Nous aimerions que toutes les sociétés favorisent le travail à distance, mettent en place des environnements de développement ouverts, affichent leur manuel d'entreprise en ligne pour que chacun y ait accès. Cette ouverture a favorisé la croissance de GitLab en tant que société. Nous allons donc continuer dans cette voie et développer cette approche. J'insiste : le modèle Zero Trust joue un rôle crucial dans notre entreprise, non seulement comme moyen de sécuriser nos actifs, mais aussi comme une métaphore de l'application de nos valeurs fondamentales.

*Mark Loveless (@simplenomad sur Twitter) est un chercheur en sécurité, un hacker et un explorateur. Il a travaillé pour des startups, de grandes entreprises, des fournisseurs de matériel et de logiciels. Il est intervenu dans de nombreuses conférences partout dans le monde – Blackhat, DEF CON, ShmooCon, RSA, AusCERT… – réunissant des hackers autour

des thématiques de sécurité et de protection de la vie privée. Il est actuellement chercheur principal en sécurité au GitLab.

(crédit photo de une © GitLab)