Conteneurs logiciels : les bonnes pratiques de sécurité

C'est en tout cas ce qui ressort du rapport « State of Open Source Security Report 2019 », selon lequel plus d'un milliard d'images Docker sont téléchargées toutes les deux semaines. C'est énorme. En fait, Docker Hub est devenu pour l'entreprise ce que l'AppStore d'Apple ou le Google Play sont pour les consommateurs. On y trouve de tout !

Les images de conteneurs que l'on peut télécharger sur le Docker Hub sont en mesure de répondre à presque tous les besoins, depuis les systèmes d'exploitation jusqu'à des écosystèmes applicatifs complets, en passant par les bases de données, les middlewares ou encore les moteurs d'applications supportant node.js, Python, et Go. En fait, les entreprises qui utilisent aujourd'hui des conteneurs (et c'est la majorité) déploient probablement des images Docker dans un environnement Kubernetes.

Et cela signifie donc qu'elles déploient probablement des images vulnérables. Car selon le rapport évoqué précédemment, « chacune des dix images par défaut les plus populaires de Docker contient au moins 30 bibliothèques système vulnérables ». Comment cela est-il possible ? Toujours selon cette étude, il est courant « que ces bibliothèques système vulnérables soient disponibles dans de nombreuses images dockers, car elles reposent sur une image mère qui utilise généralement une distribution Linux comme base ».

Un grand nombre d'images vulnérables sont ainsi téléchargées en permanence par les entreprises. Et toujours selon le même rapport, le nombre de vulnérabilités découvertes dans les trois principales distributions Linux augmente régulièrement, ce qui a pour conséquence d'augmenter mécaniquement le nombre de vulnérabilités au sein des conteneurs téléchargés, car les bibliothèques système utilisées proviennent évidemment d'une distribution Linux !

Il n'est donc pas surprenant que l'éditeur Tripwire, dans son rapport « 2019 State of Container Security » ait observé que 60 % des personnes interrogées ont connu un incident de sécurité lié aux conteneurs au cours des douze derniers mois. C'est un taux proprement ahurissant !

Mais il y a plus surprenant : dans près d'un cas sur cinq (17 %), l'organisation était consciente des vulnérabilités, mais les a quand même déployées. Et cela en dépit du fait que pour 44 % des images Docker que l'on savait vulnérables, une version plus récente et plus sécurisée était disponible. En d'autres termes, le simple fait de mettre l'image à jour aurait atténué le risque. Et en prime, 22 % de ces images auraient pu être corrigées sans mise à jour, mais tout simplement en reconstruisant l'image.

C'est incroyable, c'est déprimant, et pourtant, c'est la réalité…

Quand on dit qu'il faut « déplacer la sécurité vers la gauche » (lire : au plus près du démarrage du projet), on parle tout autant de déployer les services de sécurité appropriés au plus tôt (défense contre les bots malveillants, pare-feu applicatif Web, contrôle d'accès…) que de suivre les bonnes pratiques de sécurité tout au long du cycle de vie du projet, jusqu'à sa mise en production.

Et les bonnes pratiques en question comprennent, entre autres, une analyse des vulnérabilités… et leur correction ! (Cette dernière partie en gras est pour les 17 % qui avaient connaissance des vulnérabilités d'une image Docker, mais qui l'ont déployée sans y remédier…)

On peut évidemment faire mieux que ça. Oui, la vitesse est importante, mais la vitesse sans sécurité est dangereuse, non seulement pour l'entreprise, mais aussi pour les clients qui utilisent les applications.

Voici donc quelques bonnes pratiques de sécurité pour déployer les conteneurs en toute confiance :

1. Évaluer l'usage. De nombreuses organisations ne sont pas encore conscientes de l'omniprésence des images de conteneurs tierces dans leur système d'information. Avoir de la visibilité sur ces usages est un premier pas important, car il est évidemment impossible de traiter les vulnérabilités dans des logiciels dont on ignore même l'existence.

2. Standardiser. Il faut rechercher un terrain d'entente entre le développement et les opérations, et uniformiser pour avoir recours au moins d'images/composants différents possibles. Cela répartira mieux la charge de sécurité à travers l'organisation et se traduira en fin de compte par une meilleure sécurité pour tous.

3. Auditer le code tiers. Si des composants ou des scripts tiers sont intégrés dans les développements (et c'est presque toujours le cas), il est nécessaire de les auditer et une fois validés de les mettre à disposition à partir d'un référentiel privé.

4. Auditer les conteneurs. De la même manière, les images de conteneurs tierces devraient être vérifiées et certifiées, puis mises à disposition à partir d'un référentiel privé.

5. Faire une veille sécurité. Il est important de s'abonner aux canaux de diffusion des alertes de sécurité pour les composants tiers utilisés dans les développements. Le savoir, c'est le pouvoir…

Crédit photo : Andrii Stashko via Visualhunt.com / CC BY-NC-ND