Sécurité des applications : accélérer ou périr

Il y a quelques années, c'est à peine si on savait ce que » DevOps » signifiait. Le cloud en était à ses balbutiements, les développeurs essayaient de fonctionner comme une équipe agile, en intégrant toujours davantage de nouvelles fonctionnalités (mais surtout des correctifs !) chaque semaine.

On se moquait des équipes qui travaillaient sur des cycles de mis à jour de six mois et qui nous accusaient d'être imprudents en continuant d'agir ainsi. Dans tous les cas, notre équipe de sécurité se demandait ce que nous pouvions bien publier avec la volonté de contrôler cela.

Nous sommes en 2020 et les choses ont bien changé. Non seulement le rythme de développement a augmenté de façon exponentielle, mais les organisations ont de plus en plus misé sur leur logiciel pour se différencier de la concurrence. Pourtant, dans cette course à la création de valeur ajoutée, les équipes de sécurité ont repoussé leurs limites.

A l'époque, les équipes de sécurité n'avaient qu'à s'assurer que les serveurs étaient patchés et que le pare-feu était bien mis en place, et vérifier les applications tous les six mois au mieux pour détecter les vulnérabilités. Elles avaient construit un mur autour des applications, et peut-être même qu'elles avaient ajouté un VPN pour interdire l'accès aux mauvais acteurs.

Alors, qu'est-ce qui a vraiment changé ? Aujourd'hui, nous avons divisé nos applications monolithiques en douzaines de micro-services, chacun avec sa propre pile technique (il est préférable de laisser les développeurs choisir).

Maintenant, les changements vers ces microservices se font toutes les heures en espérant que cela va déclencher un pipeline qui permettra la mise en production de ces applications. Nous faisons maintenant tourner les applications dans des conteneurs que les développeurs choisissent au sein d'une plate-forme d'orchestration dans le cloud.
En plus de cela, nous pouvons ajouter des solutions de cloud computing telles que le stockage de fichiers, la messagerie et exposer un tas d'API à des applications mobiles de nos partenaires (au revoir VPN !).

Vous voyez où je veux en venir, il y a encore beaucoup de travail à faire.

À ce stade, nous devrions envisager une alternative. Calmer le jeu et faire le point. C'est accélérer ou périr. Notre situation est identique à celle de la grande distribution. Dans ce secteur, certaines des marques les plus anciennes et les plus respectées luttent pour survivre face à leurs homologues numériques. Elles prennent du retard sans devenir pour autant plus agiles. Il y a une conclusion inévitable.

Aujourd'hui, une marque ne vous mènera pas loin, vous devez accélérer votre développement pour être compétitif, ou votre entreprise rejoindra les dizaines de marques déjà présentes dans le cimetière des entreprises.

Qu'est-ce que cela signifie pour la sécurité des applications ? Nous savons que les applications sont

la cause la plus courante des atteintes à la sécurité des données, et nous devons donc nous assurer que nous faisons tout ce qu'il faut pour les sécuriser.

Cependant, les applications Web sont complexes. Elles sont construites sur un mélange de technologies, ont tout un tas de vulnérabilités (quelle que soit la langue) et elles doivent s'adapter quotidiennement ou toutes les heures. Dans le passé, nous avons adopté l'approche consistant à tester nos applications et à les doter d'un pare-feu d'application Web (WAF), mais ces approches exigeaient beaucoup de temps et d'expertise. Elles sont coûteuses et s'apparentent beaucoup à des produits de base.

Vous pourriez essayer de contourner cela en formant vos développeurs à la sécurité. C'est une stratégie que je préconiserais toujours dans une certaine mesure, mais elle est basée sur l'espoir et il est encore trop facile de se tromper.

Face à la complexité, il y a toujours eu une approche cohérente adoptée par les ingénieurs pour comprendre ce qui se passe à l'intérieur : l'instrumentation. Pensez à un avion, une usine ou même votre voiture familiale, les capteurs sont déployés partout pour fournir des informations sur le fonctionnement du système de l'intérieur.

C'est la même chose avec les logiciels. Il est de loin préférable de déployer des capteurs à l'intérieur d'un logiciel pour effectuer une analyse sécuritaire continue de l'application. Les développeurs bénéficient d'un retour d'informations continu, rapide et fiable dans un langage qu'ils comprennent. De plus, ils sauront s'ils utilisent des bibliothèques vulnérables et s'ils peuvent bloquer les attaques sur les applications qui auparavant faisaient cruellement défaut aux pare-feux des applications web.