Non, les startups ne sont pas les moins avancées en cybersécurité

Maillon faible de la sécurité, les startups ? On entend souvent que ce serait le cas, par manque de sensibilisation ou de budget. Et pourtant, de nombreuses startups passent très bien l'épreuve des pentests, ce qui n'est pas le cas de certaines sociétés plus établies sur le marché.

Temps de lecture : minute

---

26 décembre 2021

Article initialement publié le 29 novembre 2021

Il est temps de casser ce préjugé selon lequel les grandes entreprises seraient bien mieux protégées des cyberattaques que les startups. Le relativement bon niveau de sécurité que nous constatons chez un certain nombre de startups repose sur plusieurs aspects factuels :

Les startups sont des sociétés jeunes, développant un produit " from scratch " à partir de technologies récentes

Le fait que le produit n'ait que quelques années permet de choisir des technologies modernes, et de bénéficier de l'évolution des bonnes pratiques de sécurité pour les équipes de développement. A contrario, des entreprises plus anciennes ayant un existant technique plus conséquent rencontrent parfois de réels problèmes pour faire évoluer leur code et mettre à jour certains composants utilisés.

Dans le pire des cas, une startup ayant fait de mauvais choix techniques

pourra développer une nouvelle version de sa plateforme sur une autre stack technique, sans que cela soit aussi impactant que pour une entreprise dont le produit a 20 ans d'existence.

La plupart des startups (digitales) ont une vraie culture technique

Cela constitue un point fort majeur des startups, pour recruter des profils techniques et développer un produit réellement performant. Et cela multiplie les chances d'avoir en interne certaines personnes sensibilisées aux problèmes de sécurité, ce sujet étant " tendance " donc de plus en plus mis en avant au cours des formations initiales et des conférences techniques.

La culture technique de nombreuses startups signifie qu'elles investissent sur les aspects techniques, en donnant du poids et des moyens à l'équipe de développement. En conséquence, elles recourent moins souvent que d'autres entreprises à l'externalisation pour leurs projets de développement, ce qui permet de mieux contrôler la qualité de ce qui est produit. Elles ont aussi moins de risques qu'une application soit mise en ligne en échappant à tout contrôle, par exemple après avoir été développée par un tiers à la demande d'une équipe métier, sans collaboration avec l'équipe technique.

Les startups contractualisent avec des grands-comptes, pour vendre leur solution ou établir des partenariats

Le fait de travailler avec des grands-comptes implique que les startups sont soumises à des exigences fortes sur la cybersécurité. En effet, les processus d'achat des grands-comptes amènent les startups à devoir fournir dès le départ des gages de sécurité : questionnaires, plans de

réponse à incident, rapports de pentest… Il s'agit d'une contrainte externe très forte, qui peut vite devenir structurante pour certains aspects techniques et fonctionnels du produit. De plus, le fait de devoir passer un premier pentest pour pouvoir décrocher un contrat prestigieux amène ensuite des prises de conscience voire un intérêt spécifique de l'équipe, en fonction des résultats du pentest. C'est souvent la première étape de la mise en place d'une culture interne de la sécurité.

On remarque aussi que de plus en plus de startups se font certifier ISO27001, afin de pouvoir attester de la mise en place de cette culture de la sécurité, qui concerne de nombreux aspects opérationnels de leur activité.

Les startups évoluent dans des marchés concurrentiels et se retrouvent sous le feu des projecteurs lorsqu'elles lèvent des fonds

La visibilité et l'exposition médiatique sont des facteurs de risque. En particulier, lever des fonds peut éveiller l'intérêt de la concurrence autant que celui de hackers malveillants en recherche de cibles, pour des raisons financières ou autre. Les startups qui lèvent de fonds sont donc amenées tôt à se poser des questions de sécurité.

Cela a pour impact de commanditer des pentests dès le début de leur développement, donc de corriger tôt les vulnérabilités ayant pu être détectées. C'est un atout majeur pour se développer sur des bases saines, et être ensuite capable de répondre aux enjeux croissants de sécurité (que ce soient les attaques ou les demandes des clients et des investisseurs).

Loin d’être réticentes aux audits de sécurité, les startups ont simplement des besoins d’accompagnement plus agiles

L’idée reçue que les startups ne sont pas demandeuses d’audits de sécurité ne passe pas l’épreuve des faits, et nous venons d’évoquer plusieurs raisons à cela. Ce que nous constatons cependant, en tant que spécialistes du pentest, c’est que les startups créent des besoins de sécurité plus agiles. Le rythme des développements nécessite des feedback réguliers, au fur et à mesure des nouvelles mises en production. Bien souvent, les startups sont moins demandeuses d’un audit de sécurité complet, sur tous les pans de leur système d'infomation, que d’audits sur un périmètre plus restreint, ciblant les priorités à l’instant T.

De plus, les rapports d’audit doivent être concrets et apporter une valeur immédiate en termes d’amélioration concrète de la sécurité de leurs systèmes et de leurs produits. Le niveau de détail des recommandations de corrections doit être en phase avec cette exigence. C’est une condition pour que les développeurs acceptent le feedback et se l’approprient en le répercutant sur leur code. Dans certains cas, le feedback doit être en temps réel afin de cadrer avec les contraintes, et il doit toujours être directement exploitable.

L’autre besoin des startups concernant les résultats de pentest est de pouvoir les valoriser directement auprès de tiers (clients, prospects, partenaires). Là aussi, cela implique qu’une partie des livrables soit spécifiquement adaptée à cet objectif. Plutôt que de tirer la sécurité vers le bas, les startups au contraire font évoluer les besoins pour les adapter aux exigences de l’économie numérique.

Anne-Fleur Schoch, CEO Vaadata

Article écrit par Anne-Fleur Schoch