DevSecOps : cultiver la sécurité au cœur du développement agile

Le DevSecOps souligne l'importance de la sécurité tout au long du cycle de vie du développement logiciel. Ce mouvement était l'objet d'une table-ronde lors d'un événement organisé par Bpifrance et Axeleo.

Temps de lecture : minute

6 décembre 2023

Bpifrance et Axeleo organisaient mardi 28 novembre un événement au Hub avec l'objectif de sensibiliser l'audience à la transition vers le DevSecOps et de contribuer à la création d'un écosystème dynamique sur ces enjeux. Dans la salle, un public composé de CTO et CISO (Chief Information Security Officers). L'événement cyber, centré sur l'agilité et l'efficacité opérationnelle, a rassemblé des experts de renom tels que Stéphane Jourdan de Snyk, Luc Delsalle de Tenable, Zakaria Rachid de Believe (ancien CISO de Leboncoin.fr) et Mathieu Breton, CTO et CISO de Swan.

Dans une brève introduction de Tuan Tran, investisseur au sein du fonds digital venture de Bpifrance, l'accent a été mis sur l'intérêt croissant du fonds pour les startups et scaleups tech et deeptech. *"La cybersécurité est une priorité en raison de son caractère stratégique*", a-t-il lancé avant d'évoquer quelques-uns des deals récents du fonds, mettant en lumière des entreprises telles que GitGuardian pour la sécurité du code, Ubble pour la vérification d'identité, Mantra pour la lutte contre le phishing, et Dfns pour la conservation d'actifs pour illustrer l'engagement à soutenir des initiatives variées dans le domaine de la cybersécurité, reflétant ainsi la diversité des enjeux et des solutions dans ce secteur stratégique.

Une affirmation étayée par Mathieu Viallard, cofondateur d'Axeleo, fonds early stage spécialisé dans la B2B tech (date en entreprise, infrastructure, fintech et cybersécurité) qui insiste sur le caractère acyclique des enjeux de cybersécurité, affirmant que les budgets qui leur sont consacrés sont en constante croissance, indépendamment des fluctuations économiques et dans le contexte international. Il en veut pour preuve l'accompagnement d'Axeleo envers certains entrepreneurs du prestigieux panel d'intervenants.

Le DevOps au coeur du développement des startups

Tous se sont mis d'accord sur l'importance croissante des startups qui, par leur nature agile, adoptent les pratiques DevOps pour le développement de leurs produits. Cela a créé une dynamique nouvelle dans le domaine de la Sécurité des Systèmes d'Information (SSI), soulevant la question cruciale de ce que la SSI peut apprendre de ces approches novatrices.

Zakaria Rachid, en tant que CISO, a partagé son expérience, mettant en évidence les écueils et les silos présents dans une organisation IT traditionnelle. L'accent a été mis sur la nécessité de décloisonner les équipes pour favoriser l'innovation au sein des organisations adoptant les principes DevOps. "*Si on regarde des entreprises comme Qonto, Doctolib, Leboncoin, deux tendances se dégagent. Certains peuvent se prévaloir d'équipes transverses avec des personnes pluridisciplinaires, à l'inverse, d'autres organisations sont un peu plus 'silotées'",* a-t-il dissocié.

Mathieu Breton enchérit en mettant en avant le fait que la majorité des startups adoptent une logique de DevOps par conception, motivée à la fois par des impératifs de performance, de vélocité, et de maintenance. Il a rappelé que les infrastructures, à l'origine résultat d'opérations

manuelles, ont été standardisées avec des revues et des pratiques de surveillance pour prévenir d'éventuelles erreurs. "*Intégrer la sécurité dans le tunnel de développement faisait déjà un peu partie du fonctionnement, mais pour ce faire, il faut responsabiliser le développeur. On lui demande généralement de surveiller les métriques pour éviter de perturber la production, mais on lui demande également d'être vigilant sur les aspects sécuritaires de ce qu'il produit. Cela passe également par des vérifications SaaS, des tests DAST et des scans de vulnérabilité*", a-t-il expliqué, mettant en avant une logique de sensibilisation des développeurs dans ce processus de développement agile et sécurisé.

Le security Champion et la matrice de tests

Au cours de la table-ronde, une attention particulière a été portée au rôle crucial des Security Champions, acteurs essentiels de cette transformation. Luc Delsalle de Tenable en a esquissé un portrait : "*C'est avant tout un développeur qui connaît les contraintes, les difficultés, les délais de livraison, mais il manifeste un véritable intérêt pour la cybersécurité au point d'être prêt à investir du temps pour aider ses collègues à intégrer des principes de sécurité dans leur développement. Il travaille en proximité avec les équipes de sécurité, quand il n'est pas directement intégré à celles-ci. Ils les sensibilisent aux contraintes de développement et rendent leurs politiques plus digestes et vice-versa. Ils tirent tout le monde vers le haut*".

Stéphane Jourdan de Snyk a ajouté une dimension cruciale en soulignant que, pour tendre vers le DevSecOps, il était impératif de mettre en place une matrice de tests judicieusement élaborée pour déterminer quoi tester à des moments clés du développement. "*Cela va de l'analyse de sécurité de la bibliothèque open source utilisée initialement au test de l'infrastructure finale. L'idée est de tester la sécurité de chaque composant le plus tôt possible et constamment tout au long du développement, à savoir : les dépendances, les layers (les différentes*

couches du logiciel, ndlr), l'image source... Lorsque quelque chose est détecté, il faut en notifier le développeur - dans son langage - pour qu'il puisse apporter les modifications nécessaires dans une logique Shift Left. Plus tôt l'équipe sécurité prévient le développeur des risques, moins elle aura à éteindre des feux par la suite."

Une mutation qui limite les coûts et structure l'organisation

Luc Delsalle de Tenable n'a pas manqué de rappeler à l'audience que l'approche DevSecOps contribue à éviter des coûts potentiels en identifiant et en corrigeant les problèmes de sécurité plus tôt dans le processus de développement *"Pour la sécurité et les chefs de projets, si on détecte, en bout de chaîne, une anomalie qui touche à la base de l'infrastructure, comme la dépendance à un logiciel, l'usage d'une librairie obsolète, etc, c'est une catastrophe. On perd évidemment du temps, mais aussi beaucoup d'argent."* Une analyse appuyée par une étude du National Institute of Standards and Technology (NIST), selon laquelle le coût d'une vulnérabilité détectée au moment de la production est estimé jusqu'à 4 fois plus élevé par rapport à celle identifiée et corrigée pendant les phases précoces du développement.

Zakaria Rachid de Believe et ancien CISO de Leboncoin.fr y trouve un autre avantage, la structuration de l'organisation. *"L'humain est au cœur du mouvement qui s'opère. C'est un changement de paradigme. Elle permet à tout le monde de se rencontrer et de se responsabiliser", a-t-il déclaré.*

À l'issue d'une exploration approfondie du DevSecOps, dévoilant ses avantages, ses défis et ses bonnes pratiques, les conférenciers ont conjointement encouragé les participants à propager la culture de la sécurité à une échelle plus vaste, préconisant, dans un premier temps, de

mettre à l'épreuve l'appétit ou l'aversion au risque au sein de la hiérarchie de leur organisation et en lumière les valeurs ajoutées, surtout si leur proposition de valeur est intimement liée à la cybersécurité et qu'ils envisagent de lever des fonds.

À lire aussi
“SaaS fatigue” : comment la multiplication des logiciels favorise l’épuisement professionnel

Article écrit par Astrid Briant