avis d'expert

Le développement logiciel, nouvelle frontière de la cybersécurité

Dissocier, comme souvent, développement et sécurité apparaît désormais comme une imprudence coupable. Face aux risques croissants liés aux vulnérabilités applicatives, il convient de changer d'approche et de placer la cybersécurité au cœur même des projets. Pour accomplir ce changement culturel, le développement peut s'inspirer de la rigueur avec laquelle il traite les enjeux fonctionnels et la qualité du logiciel.

Avec le digital, les entreprises connaissent une croissance exponentielle de leur patrimoine applicatif et, mécaniquement, de leur surface d'exposition aux cyber-menaces. Et plus la numérisation gagne le cœur de métier, plus les risques – et les impacts – sont élevés, car les données manipulées sont de plus en plus sensibles et donc de plus en plus convoitées.

Face à des hackers nombreux, habiles et déterminés, les protections périphériques ne suffisent pas et les applications se doivent d'être nativement sécurisées.

Pourtant, aujourd'hui encore, bien des équipes de développement n'accordent qu'une attention distante aux enjeux de sécurité, focalisant leurs efforts sur les fonctionnalités et l'expérience utilisateur. La sécurité se résume parfois à la présence du RSSI au lancement du projet, puis à quelques tests et audits trop tardifs pour qu'il soit possible d'assurer la sécurité des applications avant la mise en production. Bien des raisons peuvent expliquer cette situation : défaut de formation des développeurs, rareté des compétences spécialisées, cloisonnement des organisations…

"L'attention apportée à la cybersécurité lors du développement doit s'inscrire dans une démarche de bout en bout, depuis la conception jusqu'à la mise en production, en passant bien sûr par les tests."

Yves Le Floch
Directeur commercial cybersécurité
Sogeti France

Une dette de sécurité

La conséquence est que les développeurs apprécient mal certains risques qui ne leur sont pas familiers, comme la prise de contrôle des bases de données par une exploitation malveillante de l'interface utilisateur, et qu'ils omettent souvent des contrôles indispensables, par exemple pour prévenir les attaques de type injection via des champs de saisie. Or, en ne tenant pas compte des risques principaux, en n'intégrant pas les mesures appropriées dès l'origine, au sein même du code, ils contractent en quelque sorte une dette de sécurité qui un jour, à travers ses conséquences et la complexité des correctifs à apporter, se paiera extrêmement cher.

Pour renforcer la sécurité des applications sans faire exploser le coût des projets, la solution est d'accorder la même attention à la sécurité applicative qu'aux questions fonctionnelles et, pour cela, de s'inspirer de la façon dont celles-ci sont traitées tout au long du processus de développement. Tout en amont, on commence donc par une analyse de risques visant à évaluer la nature et l'ampleur des risques liés à l'application afin d'établir des spécifications de sécurité, puis de dimensionner (et chiffrer) les efforts à fournir.

Accompagner les développeurs

Au cours de la phase de développement, le principal enjeu va être d'accompagner les développeurs sur un sujet auquel, on l'a vu, ils ne sont pas toujours sensibles et qu'ils maîtrisent mal. Pour cela, on injecte les questions de cybersécurité dans leurs démarches habituelles, par exemple dans le planning poker ou le backlog du processus agile. De cette façon, la sécurité est moins perçue comme une contrainte que comme une extension de la rigueur dont ils font déjà preuve vis-à-vis des exigences et bugs fonctionnels.

Pour favoriser ce qui est autant une évolution culturelle qu'une montée en compétences, l'outillage joue aussi un grand rôle. À l'image du guide OWASP, il existe des guides de cybersécurité, mais l'enjeux essentiel est de personnaliser les règles de sécurité en fonction des enjeux propres à l'application ou à l'entreprise, et des problèmes récurrents mesurés par les tests de sécurité. Guidé et sensibilisé, le développeur constate très vite l'amélioration de son code et ses propres progrès. Collectivement, c'est tout le développement qui gagne en maturité en intégrant de bonnes pratiques, par exemple le respect des règles de codage sécurisé et la rigueur dans l'emploi de briques open source.

La phase de test comporte ensuite des tests statiques, où l'on vérifie l'absence de failles dans le code, puis des tests dynamiques pour s'assurer de la sécurité de l'application en fonctionnement. Là encore, l'outillage est très important, car un outil de test de sécurité mal conçu ou mal exploité fournira de très nombreux faux positifs, ainsi que des faux négatifs, qui réduiront à néant l'effort de l'équipe de développement, voire la découragera. Les tests de sécurité professionnels et « à la demande », qu'ils soient fournis par une équipe mutualisée d'auditeurs internes ou par un prestataire externe, sont clairement la clé du succès.

Étendre au cloud l'exigence de sécurité

En matière de sécurité, l'entreprise doit avoir la même rigueur vis-à-vis des ses ressources externes que de ses développements internes. Concernant les plateformes de cloud public, on veillera tout particulièrement à la configuration de l'environnement, aux paramètres de déploiement et à la gestion des identités et des droits d'accès. Quant aux applications en mode SaaS, elles peuvent conduire les utilisateurs à mettre imprudemment des données sensibles dans le cloud, hors de tout contrôle ; on pourra alors s'appuyer sur des outils de type CASB (Cloud Access Security Brokers) et CSPM (Cloud Security Posture Management) pour filtrer et contrôler l'utilisation du cloud, et s'assurer qu'il est conforme à la politique de sécurité de l'entreprise.

Enfin, après le déploiement, un suivi des performances de sécurité sera assuré au niveau de la direction de projet ou de programme afin de corriger les vulnérabilités résiduelles au fil des versions, de prendre en compte l'apparition de nouveaux risques et d'identifier les points d'achoppement sur lesquels insister.

Une démarche de progrès

Pour être pleinement efficace, l'attention apportée à la cybersécurité lors du développement ne peut cependant rester une initiative isolée. Les efforts doivent s'inscrire dans une démarche de progrès globale et pérenne, donc portée au plus haut niveau de la DSI. Un sujet comme le RGPD, par exemple, peut contribuer à cette prise de conscience à l'échelon managérial, indispensable pour financer le surcoût des projets, inscrire le changement culturel dans la durée et mettre en place des outils et des services mutualisés. On peut ainsi constituer une équipe d'experts, dotés d'une double compétence sécurité et développement (des profils d'auditeurs de sécurité, par exemple), qui pourra venir en appui sur les points les plus délicats.

La même démarche doit être adoptée dans les méthodes de type DevOps, qui deviennent DevSecOps lorsque la sécurité est prise en compte au même titre que les impératifs de développement et d'opération.

À la fois systémique et opérationnelle, une telle approche peut permettre de réduire rapidement, drastiquement et à moindre coût les vulnérabilités applicatives. Ces failles, qui aujourd'hui se comptent parfois par centaines, sont autant d'épées de Damoclès au-dessus des entreprises et de leurs clients. S'en débarrasser, c'est faire plus que se prémunir : c'est bâtir une confiance qui, dans le monde digital, apparaît comme un différenciateur décisif.