PROVENRUN : l'expert du Security by Design

Dominique Bolignano, président et fondateur de ProvenRun, revient sur l'approche avant-gardiste en matière de sécurité adoptée par son entreprise. Il nous en dit plus sur cette démarche, les solutions proposées et les ambitions de croissance. Rencontre.

Dominique Bolignano

Quel est le métier de ProvenRun ?
Dans le domaine de la cybersécurité, il y a deux approches complémentaires. La première consiste à réagir suite à une attaque puis à mener des actions correctives. La seconde est une approche préventive pour anticiper, limiter, voire éviter les attaques. On parle alors de security by design ou sécurité par construction. C'est cette seconde approche qui est notre cœur de métier.
Très souvent, les systèmes sont conçus sans intégrer la dimension sécurité. La seule option restante pour la sécurisation de ces systèmes est de faire de la sécurité par réaction, ce qui limite le niveau de sécurité que l'on peut atteindre. Nous prenons la démarche inverse en intégrant la sécurité dès les premières phases d'un projet et du design d'un système pour que son état soit le plus proche de l'inviolabilité. L'idée est de rendre une cyberattaque contre ce système difficile au point que les attaquants n'aient aucun modèle économique valable pour l'attaquer.
J'ai créé la société il y a maintenant onze ans. Pendant les sept premières années, nous avons eu une phase de développement des produits que nous avons ensuite certifiés. Depuis deux ans et demi, nous commercialisons notre solution.

Plus concrètement, quelle est votre approche de la cybersécurité ?
Au cours des dernières décennies, nous sommes passés d'attaques dites physiques ou de proximité, qui n'avaient pas de modèle économique très intéressant pour les attaquants, à des attaques dites logiques et distantes qui peuvent prendre différentes formes : prise de contrôle de véhicules, d'avions, ou de trains à distance ; coupure d'un réseau d'énergie ; attaque contre des centres hospitaliers… En ayant recours à ce type d'attaques, les cyberattaquants peuvent, par exemple, faire chanter un fabricant automobile en le menaçant d'attaquer une gamme de véhicules contre une somme d'argent. Plus particulièrement, sur ce type d'attaques, les cybercriminels ne prennent aucun risque, parce qu'il est quasi impossible de les tracer.
Dans un monde où toutes les nouvelles infrastructures numériques s'appuient sur l'informatique et la connectivité numérique, l'enjeu de protection et d'anticipation de la menace est clé. Notre parti pris est donc de préparer les éléments clés qui permettront de protéger les architectures existantes, mais aussi les prochaines générations (cloud, IoT, systèmes embarqués…). De manière générale, ces attaques exploitent des erreurs au niveau des spécifications, de la configuration, de l'initialisation, mais essentiellement des erreurs d'implémentation (les bugs). Les cyberattaquants essayent d'identifier des bugs pour les combiner et mener des attaques. Pour réduire ce risque, il faut que la base de confiance du logiciel soit exempte de bugs, et plus généralement d'erreurs. Or, il s'agit là d'un problème de génie logiciel et informatique qui ne peut pas être solutionné par des approches traditionnelles. Tous les analystes et les études montrent qu'il y a un plancher de verre sur les systèmes complexes et le nombre de bug : à partir d'un certain niveau de qualité, à chaque fois qu'on corrige un bug, il y a une forte probabilité de rajouter un nouveau bug.
La seule technique qui permet d'obtenir zéro défaut est la preuve formelle, c'est-à-dire

"Notre parti pris est donc de préparer les éléments clés qui permettront de protéger les architectures existantes, mais aussi les prochaines générations."

“Nous visons 50 à 100 % de croissance annuelle chacune des trois à cinq prochaines années. Pour atteindre notre objectif, notre principal enjeu est le recrutement de personnel à haut potentiel, ainsi que la formation et l’intégration de nouvelles compétences. C’est un axe clé pour conserver notre leadership sur ces sujets.”

la preuve mathématique que la base de confiance est très proche du zéro bug. Pour les systèmes complexes, il s’agit de prouver que tous les chemins d’exécution ne présentent aucun problème de sécurité. Cela revient à faire des tests symboliques et exhaustifs par preuve, un niveau d’exhaustivité qui ne peut pas être obtenu avec des techniques habituelles de test.

C’est à ce niveau que nous nous différencions : nous appliquons la preuve de programme pour sécuriser les briques essentielles d’une architecture de sécurité (OS, hyperviseur ou noyau). Vient ensuite la sécurisation des autres applications qui est une démarche beaucoup moins complexe. Il nous a fallu sept ans pour développer cette approche et la faire certifier. Nous sommes ainsi le premier acteur mondial à avoir conçu un système d’exploitation avec sa base de confiance prouvé : ProvenCore. Et pour ce produit, nous avons atteint le plus haut niveau de sécurité jamais atteint pour un OS. En parallèle, nous construisons aussi des composants qui peuvent être utilisés pour la sécurisation de n’importe quelle architecture dans le monde.

Nous proposons donc des briques logicielles manquantes pour développer des architectures de sécurité ouvertes et modernes. Cette capacité à combiner la preuve formelle et un très haut niveau de cybersécurité nous différencie sur le marché.

Comment intégrez-vous les évolutions rapides et intenses connues par le secteur de la cybersécurité ?

Nous nous sommes toujours inscrits dans une démarche d’anticipation. Dans ce cadre, nous accompagnons de grands acteurs du domaine comme Azure (Microsoft) ; de grandes entreprises de l’aéronautique (Safran) ; des fabricants de composants ; des opérateurs de télécommunications (Orange, Tata Communication Inde)…

Ils viennent avant tout chercher une solution d’architecture sécurisée pour protéger leurs systèmes contre les attaques distantes que j’ai précédemment mentionnées. D’autres entreprises viennent chercher des briques pour renforcer leur architecture ou pour bénéficier d’un accompagnement afin de résoudre plus rapidement et efficacement leurs problématiques.

Quelles sont vos perspectives de croissances et vos enjeux ?

Nous visons 50 à 100 % de croissance annuelle chacune des trois à cinq prochaines années. Pour atteindre notre objectif, notre principal enjeu est le recrutement de personnel à haut potentiel, ainsi que la formation et l’intégration de nouvelles compétences. C’est un axe clé pour conserver notre leadership sur ces sujets.

Je pense que nous avons les compétences, le savoir-faire et les expertises pour conserver ce positionnement. Nous sommes convaincus de la valeur que nous apportons au monde numérique et digital au travers de nos solutions de sécurité.