Creating software that is secure by design

Developers need training and tools to elevate security as a top priority in their daily workflows

Chris Wysopal
Veracode

APPLICATIONS ARE often the way that users access and manage data, which makes application security an essential component of a broader cybersecurity strategy. If applications are not built securely, then the wrong people can access an agency's data.

To protect the wide range of technologies the government relies on, agencies are moving toward zero trust. The approach addresses security in five key areas: identity, device, network, data and application. People typically understand the importance of the first four components because they have protected them for a long time. However, application security is more complex than some of the other areas, and it involves going beyond the security team to engage the people who build the software.

It requires a shift from applying security at the end to thinking about security from the beginning and throughout the life cycle of an application, including how it is deployed and updated.

MAKING SECURITY TRANSPARENT AND INESCAPABLE

Fortunately, many agencies have begun building applications in an iterative way and automating as many steps as possible in the pipeline and in deployment. As a result, they have the opportunity to incorporate security into the development process in a variety of places as they move toward DevSecOps methodology. One crucial place to introduce security is in the testing phase.

Developers typically gather code from multiple places when building an application and run tests before they deploy it. Injecting application security into that automated testing process allows developers to understand what they're putting into production and gives them the chance to fix any vulnerabilities before deployment.

> "Vulnerabilities should be quickly detected, and the build should automatically stop **until a mitigation plan is developed and implemented.**"

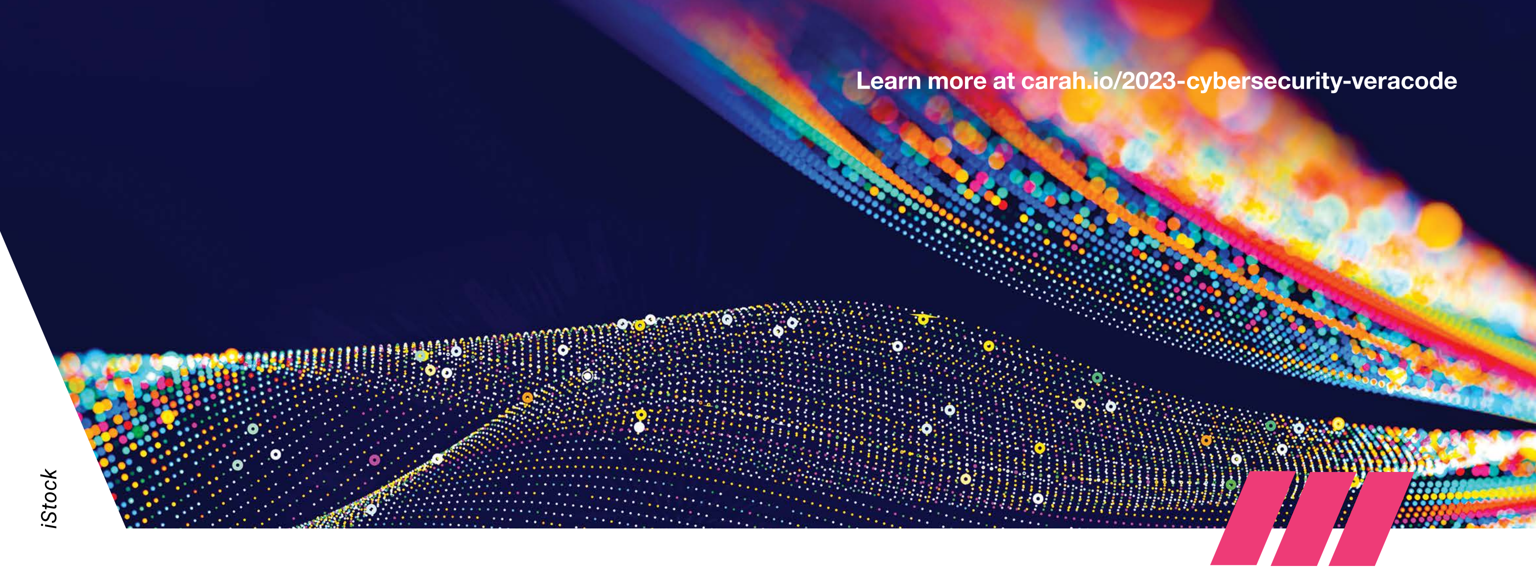
Security that works well is transparent, which means it is running in the background on every build, and it's inescapable. Vulnerabilities should be quickly detected, and the build should automatically stop until a mitigation plan is developed and implemented.

That is a minimum first step. Agencies can shift security further left by incorporating it into the developers' daily workflow so that code is scanned every time it is created or changed. In addition to finding and fixing vulnerabilities early in the process, this approach creates a feedback loop that helps developers learn.

PUTTING RESOURCES AND PEOPLE TO WORK

It's important to educate developers on how to create secure applications because many of them don't view it as part of their job. They were taught that they can build great software without thinking about cybersecurity. However, wrapping security around an application at the end doesn't work. That's why the Cybersecurity and Infrastructure Security Agency and the Office of the National Cyber Director have begun emphasizing the importance of software that is secure by design. CISA and ONCD want to ensure that companies embed security into every aspect of their software development. Agencies should do the same for the applications they create in-house.

Achieving that goal hinges on educating all developers, whether


Learn more at carah.io/2023-cybersecurity-veracode

iStock

they're government employees or contractors, and giving them the tools they need so they can incorporate security into the way they work.

Fortunately, the government has created valuable resources that focus on application security. CISA and ONCD based their guidelines on the National Institute of Standards and Technology's Secure Software Development Framework, for example. In addition, the government has knowledgeable employees. It's just a matter of putting those resources and people to work building secure software. Once agencies do that, they will achieve their desired outcomes. ■

Chris Wysopal is co-founder and CTO at Veracode.