VERACODE

What TECH FIRMS Should Know About Software Security

01

A NEW ERA EMERGES

Every business in every industry is now reliant on software to deliver products and services to business partners and customers. The novel coronavirus pandemic has turbocharged this trend by pushing more and more activity online, particularly as physical offices and stores close.

As more and more business processes and transactions shift to electronic platforms, the danger of serious cyberattacks grows. Technology firms must confront and address this challenge.

SECURE SOFTWARE IS A COMPETITIVE ADVANTAGE

Even before COVID-19 appeared and the global pandemic took root, software security was a growing concern. An overwhelming 94 percent of respondents to a recent IDG survey reported that their confidence in a vendor whose application security had been validated by an established independent security expert would increase, and 66 percent said they were much more likely to work with such a vendor.[1]

Today, as remote work becomes the norm and consumers shop, bank, and handle myriad other tasks online, security is not an abstract point. There's a growing expectation that software will perform well — without glitches, bugs, or major security flaws. With brand reputation and dollars at stake, tech firms can't afford to minimize the risk of vulnerable software.

What this means for the tech industry is that cybersecurity, and particularly application security, is critical. More than four out of five organizations "always or frequently" incorporate security requirements into a contract. In addition, 82 percent "always or frequently" evaluate the security of new applications on their personal devices. These and other factors are at the center of building trust. The ability to detect and repel potentially destructive attacks is mission critical.

WATCHING OUT FOR CRYPTO

Tech firms understand the importance of producing high quality software — it can make or break a company's reputation. But quality is more than the sum of great features and fast performance. It's also ensuring that code is secure. Unfortunately, many organizations put security, like cryptographic issues, on the back burner. According to the Veracode ***State of Software Security (SOSS) X*** report, tech firms have more cryptographic issues plaguing their code than organizations in other industries. Our data reveals that 66 percent have software vulnerabilities linked to cryptographic issues.[2] This includes broken crypto algorithms, improper validating certificates, storing sensitive information in cleartext, and employing inadequate encryption strength.

Like other security flaws, crypto vulnerabilities can lead to intellectual property theft and the disclosure of personally identifiable information, such as Social Security numbers, credit card data, and banking information. Left unaddressed, these vulnerabilities will continue to weaken an organization's security framework. Crypto vulnerabilities are frequently preventable through secure coding practices, including scanning code frequently and training developers on how to use encryption methods more effectively.

IMPROVING CREDENTIAL MANAGEMENT

Veracode's ***SOSS X*** also found that tech firms struggle with higher than average levels of credentials management vulnerabilities.[3] This type of vulnerability essentially gives cyberattackers unauthenticated, unauthorized access to sensitive files, data, and information. Poor password management practices can even lead to account takeovers. Common causes include hardcoded passwords and plaintext passwords in config files.

Prevention and remediation of this vulnerability require a focus on several key factors: secure coding practices, locking down administrative controls, and using tools such as multi-factor authentication to thwart unauthorized access to accounts. ***Dynamic Analysis*** also plays a role in identifying these types of vulnerabilities.

Our data reveals that

66%

of apps at tech firms have crypto vulnerabilities, and

52%

have credential management problems.[4]

SAAS APPSEC AND YOUR BOTTOM LINE

In today's environment, budgets are facing intense scrutiny. ***SaaS-based application security*** can have a dramatic effect on your bottom line vs. an on-premises solution. With a SaaS-based solution, it's possible to begin scanning code on day one, without having to change infrastructure or add hardware.

For organizations that take the SaaS route, there are no maintenance costs, no ongoing operational issues, and more accurate and dependable results. It's also easier to manage spikes in demand for services without being forced to budget for redundant systems and maximum availability.

Real-Life Spotlight

AUTOMATION ANYWHERE USES SECURITY AS A COMPETITIVE ADVANTAGE

Automation Anywhere, a global enterprise software firm, recognized that without stringent security, its business model was fundamentally at risk. With it, however, the company could gain a competitive advantage. The firm, which offers robotic process automation (RPA) tools for Fortune 100 and Global 2000 firms in 90 countries, needed to ensure that automation bots built into its software had the protection they needed. Cyberattackers exploiting vulnerabilities in the code could cause dire consequences.[5]

To transform its application security framework, the company turned to Veracode and its *Verified program*, which is designed to help companies achieve the highest level of application security. The firm found that the program was easy to put in place, could scale in response to customer requirements, and could prove to customers and prospects, at a glance, that security was a priority for Automation Anywhere. The company achieved Verified Continuous status, Veracode's highest security level. In 2019, the firm launched a new *web-based cloud-native RPA system*. With security tools now integrated into development workflows and automated application security testing that offers real-time results, dynamic scalability, and advanced training, the company has been able to make security a major selling point, ensuring the sustainability of its business model.

CONTACT US

to find out how we can help you start or optimize your AppSec program.

VERACODE

[1] "*How to Make Application Security a Competitive Advantage,*" IDG.

[2] *State of Software Security X*, Veracode.

[3] Ibid.

[4] Ibid.

[5] "*Veracode Helps Automation Anywhere Confidently Release the First Web-Based, Cloud-Native RPA Solution,*" Veracode.

Veracode is the leading AppSec partner for creating secure software, reducing the risk of security breach and increasing security and development teams' productivity. As a result, companies using Veracode can move their business, and the world, forward. With its combination of automation, integrations, process, and speed, Veracode helps companies get accurate and reliable results to focus their efforts on fixing, not just finding, potential vulnerabilities.

Veracode serves more than 2,500 customers worldwide across a wide range of industries. The Veracode cloud platform has assessed more than 14 trillion lines of code and helped companies fix more than 46 million security flaws.

Learn more at *www.veracode.com*, on the Veracode *blog* and on *Twitter*.