SPONSORED CONTENT

CIO FROM IDG CSO FROM IDG

PRESENTED BY

VERACODE

APPLICATION SECURITY IN EUROPE'S ERA OF HIGH STAKES

Technology, and more specifically software, is the major driver of innovation and economic growth for the 21st century. Software is rapidly redefining how employees work, customers engage, and teams operate.

But while applications can provide organizations with a competitive edge, they are the most frequent incident pattern in confirmed breaches, and attacks at the application layer are growing by more than 30% annually.

In response, enterprises in Europe are ramping up efforts to ensure data privacy and secure applications. In fact, an IDG/Veracode Application Security survey reveals that 86% of European organizations evaluate and/or audit applications in use for security requirements at least once per quarter.

THE DANGERS OF SECURITY BREACHES

The good news is time spent carefully evaluating and auditing applications can pay off—tremendously. The majority (80%) of respondents report uncovering vulnerabilities at least 25% of the time. Indeed, European digital businesses faced 80 million fraud attempts in the first three months of 2018—an increase of 30% compared with the same period a year ago, according to ThreatMetrix.

For consumers, cyberattacks are precursors to identity theft and fraud. For organizations, failure to detect these vulnerabilities can lead to security breaches resulting in application downtime, application performance issues, increased operational costs associated with remediation, loss of customer data, negative press, and loss of intellectual property.

MOUNTING RISKS – AND RESPONSIBILITIES

To avoid negative repercussions, savvy organizations ensure the security of the applications they build and of those they purchase. That's because third-party applications can pose serious data security risks and expose European organizations to huge penalties and legal liabilities, especially with the recent introduction of the General Data Protection Regulation. This European privacy law raises the stakes on security by requiring companies handling the data of EU citizens to comply with strict data privacy regulations—or face dire financial consequences.

Faced with this mounting pressure to safeguard applications, European companies are placing even higher importance on assessing vendor and partner security capabilities than their U.S. counterparts.

A staggering 94% of IDG/Veracode survey respondents agree it's important to assess the application security capabilities of the vendors and partners from whom they procure software and applications. Another 84% are concerned about the potential data risk posed by applications that are developed and/or maintained by a third party. And 88% concede that if a data breach arises from the use of a third-party application and customer data is compromised, ultimately the responsibility lies with the organization itself.

DEMAND FOR KEY SECURITY CAPABILITIES

European companies are demanding potential vendors and partners deliver these key security capabilities (in order of priority):

- Evidence of ability to perform application and security testing
- Proof of testing by independent third-party testing vendor
- Demonstrated use of specific secure coding practices
- Demonstrated ability to scan and remediate vulnerabilities within open source components
- Reports from credible third-party application security tools

ROADBLOCKS AHEAD

Despite this due diligence, European companies still face plenty of roadblocks when trying to assess the security status of applications and software that they haven't developed in-house.

Get the full survey results and analysis in our report

How to Make Application Security a Competitive Advantage

In fact, European respondents more often report that software vendors, even if willing to share information, don't have the expertise to conduct testing themselves. That's a problem: it's highly important for vendors and partners to provide a variety of information regarding their security.

The use of personal devices can also present risks. In Western Europe, an estimated 64.7% of people own smartphones, according to Statista. As a result, 35% of European survey respondents always spend considerable time evaluating the security status of new applications before downloading or installing them on a personal device, while 55% perform evaluations frequently.

DRIVING ACCOUNTABILITY

Fortunately, European organizations are finding effective ways to make vendors more accountable for the security of their applications. For example, many are pushing security to the forefront of vendor and partner contract negotiations. Nearly half (43%) of respondents always incorporate security requirements into contracts and/or acceptance terms; 47% frequently incorporate them; and a mere 10% negotiate security capabilities on a case-by-case basis.

"As a European who has been living in the U.S. for the past 20 years, it's interesting to observe the differences in security approaches and philosophy between the two regions," says Mark Curphey, Vice President of Strategy at Veracode. "I suspect the differences may stem in part from Europeans being used to working across cultural and geographical boundaries. In this environment, security built into contracts and legal obligations makes perfect sense. Europe has also traditionally been more sensitive about personal privacy, something we saw mature in the form of GDPR last year."

Another approach to minimizing the security risks of third-party applications: relying on the expertise of an independent security expert. In fact, 90% of European respondents believe it's critical or very important that software security is validated by an independent security expert.

VALIDATE IT

But not all vendors embrace the same high security standards. For this reason, European organizations often look for key features in validation programs to ensure the security of critical applications. The top three components survey respondents consider highly important in an independent security validation program are:

- **Certification that the software/application code is free of security-related defects (96%)**
- **Imposed/guaranteed time restriction for remediation of future security issues/flaws (88%)**
- **Verification that the providers have integrated continuous scanning to detect vulnerabilities throughout the development process (86%)**

Not only can validation programs and security certification minimize the risk of a breach, but they can strengthen vendor relationships. In fact, survey respondents in Europe are more likely than U.S. respondents to report that security certification impacts their perception of an application provider. Case in point: three-quarters of respondents say their level of confidence in a potential vendor or partner would increase significantly if security has been validated by an established independent security expert.

All of which can be a boon for business. All things being equal, 67% of survey respondents are much more likely to consider doing business with a vendor or partner whose software has been independently verified as secure versus one whose security status is undetermined.

SECURITY FROM THE INSIDE OUT

Given today's cyberattack landscape, recognizing the vulnerabilities lurking in application code is more important than ever, in both code developed internally and code developed by a third party. Work to improve the security of your applications from inception through production, and seek out software vendors whose products are certified secure by a third party.

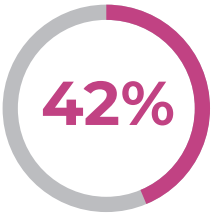
OBSTACLES THAT IMPEDE A THOROUGH STATUS CHECK

Respondents stated the following as top challenges in the face of today's complex cyberattacks and sophisticated software programs:

Security-related information is difficult to understand

Too time-consuming to review

Struggle to find the right information



Get the full survey results and analysis in our report

How to Make Application Security a Competitive Advantage