ARE YOU COMMITTING THESE

6 Common AppSec Blunders?

Software and code-related security issues are a growing concern.

74%

of senior IT and business professionals agree this is true.[1]

It's easy to see why. With technology's rapid evolution has come a slew of new security threats, making application security more critical than ever.

There are common blunders companies make with their AppSec programs. **Have you committed any of them?**

BLUNDER #1

Using Just One Testing Method

Different testing methods discover different vulnerabilities. For instance:

ENCAPSULATION THREATS FOUND IN APPS BY

Static testing **22%**[2]

Dynamic testing **39%**[3]

Deployment configuration was one of the top three vulnerabilities identified by dynamic testing but wasn't found by static testing at all.[4]

FIX IT: Test throughout the SDLC using different testing methods to ensure application security.

BLUNDER #2

Ignoring Open Source Vulnerabilities

In a recent study, **88% of Java applications had at least one flaw in a component**.[5]

FIX IT: Create a dynamic inventory of your open source libraries in use so you can scan and identify vulnerabilities more seamlessly.

BLUNDER #3

Not Integrating Security Testing Into The Development Process

Just 34% of companies are considered "Security Masters," or leaders in application development security that integrate security early in the development process.[6]

THESE COMPANIES SEE:

40% higher revenue growth

50% higher profit growth[7]

FIX IT: Developers should analyze their code for security and fix flaws as they're writing code in real time.

BLUNDER #4

Not Having An AppSec Policy

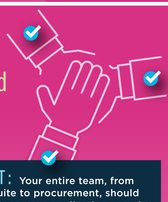
Approximately 70% of applications failed security testing when measured against major industry vulnerability standards.[8]

Mature AppSec programs have a 35% higher pass rate than new programs.[9]

FIX IT: An effective application security policy will get everyone on the same page about how to prioritize issues.

BLUNDER #5

Not Getting Everyone On Board



Only 24% of senior IT and business professionals strongly agree their organization's culture and practices support collaboration across ops, dev, and security teams.[10]

FIX IT: Your entire team, from the C-suite to procurement, should all buy in to your application security policy and ensure it's followed.

BLUNDER #6

Not Having The Right People And Tools

Lack of skills **58%**

Lack of proper tools **47%**

are considered top hurdles for companies striving to embed security into the entire software development process.[11]

FIX IT: The security skills gap is significant and growing. Consider partnering with third-party AppSec experts who can help you refine and optimize your AppSec strategy.

These blunders are extremely common and equally detrimental to companies of all sizes and across all industries.

Want to learn how to avoid these AppSec mistakes? **Download our E-book to find out.** GET THE E-BOOK

SOURCES: [1] https://freeformdynamics.com/wp-content/uploads/2018/02/2018_Software_Lifecycle_Security.pdf. [2] https://www.veracode.com/blog/managing-appsec/single-appsec-technology-not-enough. [3] Ibid. [4] Veracode, *2017 State of Software Security*, 2017. [5] Ibid. [6] https://freeformdynamics.com/wp-content/uploads/2018/02/2018_Software_Lifecycle_Security.pdf. [7] Ibid. [8] Veracode, *2017 State of Software Security*, 2017. [9] https://www.csoonline.com/article/3231084/application-security/application-security-what-s-working.html. [10] https://freeformdynamics.com/wp-content/uploads/2018/02/2018_Software_Lifecycle_Security.pdf. [11] Ibid.

VERACODE

Veracode is a leader in helping organizations secure the software that powers their world. Veracode's SaaS platform and integrated solutions help security teams and software developers find and fix security-related defects at all points in the software development lifecycle, before they can be exploited by hackers.

Our complete set of offerings helps customers reduce the risk of data breaches, increase the speed of secure software delivery, meet compliance requirements, and cost effectively secure their software assets – whether that's software they make, buy, or sell.

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