Application Security

Fallacies + Realities

WHAT'S INSIDE

VERACODE

INTRODUCTION

The news headlines have been filled with stories about security breaches in recent months.

And most of these high-profile breaches originated with a vulnerability in an application. In fact, web application attacks are the most frequent incident pattern in confirmed breaches. Yet, most organizations are not spending time or money on application security. So why the disconnect? One reason is that fallacies abound when it comes to application security. Many of these fallacies stem from the traditional, on-premises tools-based approach to application security, which has fostered the misconception that application security programs are expensive and difficult to manage. But as breaches continue to make headlines, organizations are realizing the serious risk posed by applications.

Now is the time for organizations of all sizes to understand the fallacies, and the truths, of application security.

TWEET THIS STAT

Web application attacks remain the most frequent incident pattern in confirmed breaches.

2018 Verizon Data Breach Investigations Report

APPSEC FALLACY NO. 1

Implementing an application security program is cost prohibitive

The reality

Cyberattackers are increasingly exploiting vulnerabilities in the application layer, leaving companies with significant damage and financial loss. At the same time, the movement toward cloud-based security solutions has reduced the cost of application security. With the odds of a costly breach going up, the expense of application security should no longer act as a barrier to implementing a program, as the cost of a breach outweighs the cost of the program.

The details

With the dramatic shift from on-premises application security to cloud-based, the financial picture has changed. You no longer need to hire more security experts, or install more servers or tools, to start or scale an application security program — leading to substantial cost savings in installation and maintenance compared to traditional on-premises solutions.

The cost of a breach is felt in:

LOST REVENUE

This might result from stolen corporate data, lowered sales volumes (if consumers get scared) or falling stock prices.

MONEY SPENT ON INVESTIGATION AND CLEANUP

After suffering a breach, organizations must spend time and money to identify the source of the breach (which can be a lengthy and expensive process), repair the damage and then re-secure (and possibly re-certify) the breached system. A recent joint Veracode/Centre for Economics and Business Research (Cebr) report found that cyberattacks cost UK firms £34 billion in revenue losses and subsequent increased IT spending.

COST OF DOWNTIME

When systems are down due to an application flaw, or shut down in response to a breach, the costs can soar. A recent *Information Age* article estimated that every hour of downtime costs businesses $100,000. In addition, time spent fixing a breach means time diverted away from development and innovation.

BRAND DAMAGE

The long-term reputation damage associated with security breaches can be substantial and lead to intangible costs or loss of business.

Learn More

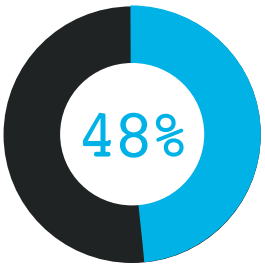
EBOOK
Making Application Security Pay

WEBINAR
The ROI of AppSec

INFOSHEET
The Advantages of a SaaS-Based Application Security Solution

WEBINAR
How to Get the Most Out of Your Application Security Program

TWEET THIS STAT



In one study, 48% of organizations report having been involved in a publicly disclosed data breach, and nearly all found that the breach had long-term negative impact to their revenues and to consumer trust.

The Global State of Online Digital Trust

TWEET THIS STAT

$6 trillion

The predicted annual global cost of cybercrime by 2021.

2017 Cybercrime Report, Cybersecurity Ventures

Simply put, spending on proactive application security today reduces the chance of a massive financial loss tomorrow.

2

APPSEC FALLACY NO. 2

Application security is highly complex

The reality

Application landscapes are complex, but securing them doesn't have to be. Rome wasn't built in a day, and your application security program won't be either. The keys are to start small, keep things simple, prove the value and then mature the program over time. The most successful companies we've worked with have started by securing a few apps at a time.

The details

You don't have to secure every app on day one. Reduce the complexity of application security by building the program in stages. You can start by implementing procedures to assess the most business-critical applications, and then scale your program from there.

At a high level, the evolution of an application security program looks like this:

PHASE 1

Start with the most critical applications

PHASE 2

Set policies and metrics

PHASE 3

Scale to assess all legacy applications and integrate in the SDLC

PHASE 4

Create a strategy for assessing third-party applications and components

With the right solution and the right game plan, application security goes from feeling very overwhelming to becoming very doable.

Learn More

REPORT
Ultimate Guide to Starting an Application Security Program

GUIDE
Everything You Need to Know About Maturing Your AppSec Program

GUIDE
From Ad Hoc to Advanced: Your Path to a Mature AppSec Program

APPSEC FALLACY NO. 3

Covering only business-critical applications is the key to success

The reality

Securing your most critical apps is a good place to start — not a good place to stop. Cyberattackers are increasingly targeting less-critical and third-party applications, meaning the entire application landscape needs to be secured.

The details

If your entire application landscape is not secured, cyberattackers have a way to access your systems and their critical information. Securing all your applications — including those you've built, bought or pieced together with in-house and open source components — is critical. Why? Because cyberattackers are looking for the path of least resistance into your organization, and that path is increasingly through less-critical and third-party applications.

Recent high-profile breaches prove this point. JPMorgan was recently breached through a website for its annual charity road race — hardly a business-critical application. Hackers found a vulnerability in this third-party website and used it to access the enterprise's network.

However, most organizations are not currently securing their entire application landscape and, in fact, don't even know how many applications they have. Application security starts with knowing what needs to be secured. You need a global inventory of all your public-facing web applications such as corporate sites, temporary marketing sites, related sites (.mail, .info, etc.), international domains and sites obtained via M&A. The security of third-party apps and components shouldn't be neglected either, as evidenced by the JPMorgan example above.

You should find an application security solution that can assess all your apps — whether they are built, bought or assembled.

Learn More

GUIDE
Your Guide to Application Security Solutions

GUIDE
Understanding your Open Source Risk

WEBINAR
How to Manage Open Source Risk Within the DevOps Delivery Model

TWEET THIS STAT

Research done by IDG revealed that almost two-thirds of applications are not assessed for security.

APPSEC FALLACY NO. 4

Application Security is only for software vendors

The reality

Every company today is reliant on applications and uses them to provide access to its critical information. Therefore, every company must also ensure its applications are secure.

The details

Mobile and cloud computing are dramatically changing the way we deliver business innovation. The world now runs on applications, and users typically interact with enterprises through applications. As a result, every company is becoming a software company — regardless of what its primary business is. And most companies today are rapidly producing web, mobile and cloud applications in order to keep up with the pace of innovation. To innovate even faster, organizations are using Agile and DevOps development processes as well as augmenting their own internal development programs by purchasing software from third-party providers and integrating open source libraries and components.

Ideally every piece of software would be assessed for security, but that isn't the reality. Research done by IDG revealed that almost two-thirds of applications are not assessed for security.

Learn More

INFOGRAPHIC
Application Security Awareness Not Aligned with Application Security Risk

4

Every company, in every industry, now runs on software and needs to make application security a priority.

APPSEC FALLACY NO. 5

Developers won't change their processes to incorporate application security

The reality

Security assessments do fit into modern development methods, provided they adapt to the these new methods.

The details

It is true that development and security had a strained relationship in the past. This is because the standard ways of assessing code for security didn't mesh with the modern methods of software development. For instance, the waterfall development process has very distinct phases, and each security activity is completed before moving on to the next phase. Agile and DevOps, on the other hand, don't have such distinct phases. And it was assumed that security assessments would slow down the constant flow of development. However, security assessments can fit within Agile and DevOps processes as long as security practitioners realize that security must adapt to development methods, not the other way around.

For instance, developers should pull security "left" into development processes and the "definition of done" rather than tacking it on at the end. Finding vulnerabilities during the coding phase instead of during a separate security hardening sprint saves time and increases velocity, while at the same time ensuring the security of the software being developed, tested and shipped.

In addition, some security solutions are better suited to working in modern development processes than others. For example, static analysis, or SAST, which can scan code for potential vulnerabilities when the software is in a non-running state, lends itself to modern development processes. This assessment technique enables developers to assess their software for issues without waiting for a running, testable application. A solution that integrates with developers' existing processes and tools is also key to coding securely today. By adding APIs to the development tools already being used by the programming teams (JIRA, Jenkins, Team Foundation Server), security can become so integrated into the development processes that it is seamless.

Learn More

WEB PAGE
Veracode Static Analysis

GUIDE
5 Principles for Securing DevOps

WEBINAR
Secure by Design

6

APPSEC FALLACY NO. 6

One single technology can secure all applications

The reality

There is no AppSec silver bullet, and a truly effective application security program uses the strengths of multiple testing techniques.

The details

Effective application security ultimately includes more than one automated technique, plus manual processes. For example, static analysis (SAST) doesn't require a fully functional system with test data and automated test suites, and dynamic analysis (DAST) doesn't require modifying the production environment. Because of these strengths, SAST can be used earlier in the development cycle than both interactive application security testing (IAST) and DAST. DAST can be used more easily than SAST and IAST in production.

Each analysis technology has its own strengths. Static, dynamic, IAST, software composition analysis, web perimeter monitoring and manual penetration testing all play a role in a complete application security program.

"Businesses aren't asking for SAST, IAST, DAST — they're asking, 'how do I solve my problem' and the right answer is, 'with a little bit of everything, depending on your environment."

Chris Wysopal, Veracode Co-Founder, CTO and CISO

Learn More

GUIDE
Your Guide to Application Security Solutions

Ultimately, effective application security is not focused on tools, but rather a systematic approach that leverages multiple technologies that, taken together, reduce application risk.

APPSEC FALLACY NO. 7

Firewalls, anti-virus and network security cover applications by default

The reality

Your organization is not secure if your applications are not. Firewalls, network security and anti-virus are not securing your apps. A dedicated application security strategy reduces risk in the area that is most likely causing the weaknesses in your infrastructure.

The details

One of the reasons that cyberattackers have turned their attention to web-facing applications is that most enterprises are proficient at hardening traditional perimeters with next-generation firewalls, IDS/IPS systems and end-point security solutions. This makes applications an appealing target, because they are:

- Exposed to the Internet, making them easy to probe by attackers from anywhere in the world.
- Replete with common vulnerabilities, such as SQL injection, that can easily be found via free scanning tools.
- Always changing, with short development cycles driven by new methodologies such as Agile and continuous deployment.
- Assembled as hybrid code from a combination of in-house development, outsourced code, third-party libraries and open source components — without visibility into which components contain critical vulnerabilities.
- Even more vulnerable with modern technologies that increase the attack surface by incorporating client-side logic using complex JavaScript or RIA technologies such as Adobe Flash.

Learn More

INFOSHEET
What is Application Security?

Of course, you still need your WAFs and your anti-virus, but application security is another critical part of your security ecosystem, and should be treated as such.

CONCLUSION

You can no longer afford to ignore application security. Every company now runs on software, and that software introduces risk. Rather than relying on application security assumptions and anecdotal evidence, you need to get the facts, and take steps toward a comprehensive application security program.

1. The odds of an expensive breach due to an application vulnerability are going up.
2. Building an application security program in stages is key.
3. Cyberattackers are increasingly targeting third-party and less-critical apps.
4. All companies are reliant on applications, and must ensure the applications are secure.
5. Security assessments do work with modern development methods, as long as they adapt to these processes.
6. There is no AppSec silver bullet — a mix of technologies is needed.
7. Firewalls, anti-virus and network security do not secure your applications.

LOVE TO LEARN ABOUT APPLICATION SECURITY?

Get all the latest news, tips and articles delivered right to your inbox.

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.

Copyright © 2020 Veracode, Inc. All rights reserved. All other brand names, product names, or trademarks belong to their respective holders.