THE IMPACT OF SECURITY ON APPLICATION DEVELOPMENT

August 2015
THE IMPACT OF SECURITY ON APPLICATION DEVELOPMENT

EXECUTIVE SUMMARY

The growth of enterprise-developed applications has made it easier for businesses to use technology to work more efficiently and productively. These enterprise applications interface and integrate with other applications, software platforms and databases used within a business, including some that are customer-facing. They can be deployed across a corporate network, Internet or Intranet.

Business demands for IT security continue to grow as more and more enterprises move their applications to the cloud and rely on partnerships with third-party software to extend and optimize their end-to-end operations. Not only are large organizations utilizing more cloud-based, SaaS products than ever before, but they are also creating applications that rely on API integrations, external data feeds and cloud services. Doing so helps the enterprise deliver more functional applications to support the business, but it also broadens the attack surface.

These applications are not only tasked with meeting complex and evolving business process goals, but they must also comply with strict security, privacy and often compliance requirements. Despite allocating millions of dollars to developing these applications, enterprises still underinvest in a critical component: securing enterprise applications against attacks. As the pace of application development speeds up and the frequency of releases increases, how are enterprises ensuring those comprehensive security needs are being met?

In an ideal world, applications would always be coded securely, pass all vulnerability scans and penetration tests, and never encounter zero-day attacks. Unfortunately, there is no such thing as invulnerable code, and in a world of rapid software release cycles, remediation is often regarded as a burdensome task that slows down the pace of business and innovation.

To understand the relationship between application development and security requirements, Prevoty surveyed more than 200 application developers on the role of security and its influence on the development process.
Key takeaways from the survey responses include:

- 85 percent say vulnerability remediation has a significant impact on the ability to release applications and features on schedule and on budget.

- More than 70 percent admitted that business pressures to release application updates quickly often override security concerns.

- Nearly 80 percent of developers worry that their clients won’t trust their applications if they admit there is a security flaw.

- Nearly half (43 percent) admit to releasing applications with vulnerabilities at least 80 percent of the time.

THE BUSINESS PRESSURES OF RELEASING SECURE APPLICATIONS

Developers are faced with business pressures to release applications, update features and fix bugs quickly. More than half of survey respondents say they have a release cycle of one week or less, regardless of development workflow methodologies such as agile, SCRUM, Crystal, etc.

In the rush to release new versions or updates to applications, more than 70 percent admitted that business pressures to quickly release applications updates often override security concerns.
THE IMPACT OF SECURITY ON APPLICATION DEVELOPMENT

**FREQUENCY OF APPLICATION RELEASES**

- **Daily:** 24%
- **Weekly:** 29%
- **Monthly:** 19%
- **Every Few Months:** 16%
- **No Schedule:** 13%

70% SAY THAT BUSINESS PRESSURES OVERRIDE SECURITY CONCERNS

In addition to business pressures, regulatory requirements also demand a developer’s attention. According to Prevoty’s research, nine out of 10 security respondents were concerned with regulatory compliance. More than half (54 percent) focused on HIPAA compliance, 42 percent focused on PCI, and more than a third focused on both SOX and FISMA.

**COMPLIANCE AND REGULATORY CONCERNS**

- **PCI:** 42%
- **HIPAA:** 54%
- **SOX:** 36%
- **FISMA:** 36%
- **Other:** 7%
- **No compliance requirements:** 11%

Furthermore, nearly 80 percent of developers worry that their clients won’t trust their applications if they admit there is a security flaw. Add the pressure of fast release cycles with the pressure to adhere to industry demands, and developers are working under multiple constraints at breakneck speeds to release new enterprise applications.

78% SAY THEY’LL LOSE CLIENT TRUST IF THERE IS A SECURITY FLAW
Since attack vectors are amorphous, constantly changing and evolving in subtle ways, developers may not be able to architect applications in ways that would prevent future, unknown attacks. How does someone who is not a hacker by nature stay ahead of never-before-seen attacks or new malware created by the hacking community? Application developers are in the business of building technology – not breaking it – so they may not always look at code in the same way that a hacker would.

RELEASING ENTERPRISE APPLICATIONS WITH VULNERABILITIES

Given short release cycles and the increase in business pressures, development teams have adapted their security practices to try to keep up with emerging threats and attacks. The practices most frequently employed are application vulnerability scans, penetration tests and dedicated in-house security resources.

According to Prevoty research, at least 82% of respondents say their companies perform some vulnerability scanning and/or penetration testing prior to application release, the research revealed something peculiar and highly alarming: applications are still being released even before all known vulnerabilities can be fixed.

To be specific, nearly half (43 percent) admit to releasing applications with vulnerabilities at least 80 percent of the time. Think about that percentage for a moment. Eighty percent of the time developers release or update a production application, they are doing so with the knowledge that they are in fact vulnerable to attack.

PERCENTAGE OF APPLICATIONS RELEASED WITH SECURITY VULNERABILITIES

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17%</td>
<td>Always</td>
</tr>
<tr>
<td>26%</td>
<td>80% of releases</td>
</tr>
<tr>
<td>11%</td>
<td>60% of releases</td>
</tr>
<tr>
<td>25%</td>
<td>Less than 50% of releases</td>
</tr>
<tr>
<td>21%</td>
<td>No releases with vulnerabilities</td>
</tr>
</tbody>
</table>
How is it that so many test and scan for vulnerabilities yet, despite these measures, openly admit that they are still releasing applications with known vulnerabilities? To understand this contradiction, it’s important to remember the business pressures of a large enterprise and the mission value of application development. After a scan takes place, it requires time, skill, patience and expertise to wade through vulnerability logs, rule out the false positives (reporting a vulnerability as present when in fact it non exists) remediate the code, re-test and re-release.

These code reviews, scans and tests can be limited in their effectiveness in servicing the true business needs of large organizations. These revelations tell us that developers want to follow best practices and comply with industry standards (or must do so for regulatory compliance reasons), using available tools to protect their applications.

The unfortunate truth is these existing tools don’t actually fix any of the vulnerabilities prior to deployment or help developers optimize their ability to detect and prevent actual malicious attacks on their production applications. Once an application is pushed into a live, runtime environment, most enterprises do not have a way of identify attacks hitting the applications so there is no view of the effectiveness of the vulnerability management program.

VULNERABILITIES AND THE SIGNIFICANT IMPACT ON THE BUSINESS

Prevoty’s research reveals that application developers at large enterprises do understand how critical vulnerability remediation is for the business and the damage caused by a data breach, but 85 percent say vulnerability remediation has a significant impact on the ability to release applications and features on schedule and on budget.

For enterprises with more than 1,000 employees, that same response jumps to a staggering 93 percent. This is a deep pain point as developers, risk organizations and IT departments are always being judged on performance - constantly juggling the ability to release secure enterprise applications on schedule and on budget.
As discussed earlier, application developers are taking the precaution of running vulnerability scans, but even the most sophisticated scanners can’t identify all potential vulnerabilities in an application. Moreover, developers may not have the skills to scope and prioritize which vulnerabilities to remediate amidst the daily pressures of the business. The fact that so many enterprises are struggling with large vulnerability backlogs and making unfavorable tradeoffs between the demands of development and security is a testament to the inefficiencies of our current application protection and vulnerability management capabilities.

Given the destructiveness of a major data breach, it should be a business priority to make sure that all known vulnerabilities are being remediated. Unfortunately, at this time, the burden of the remediation process does not align developers with application security. Instead, it poses a threat to the goal of delivering business value to the organization at large.
CONCLUSION

The application development process is rife with security perils. From competing business pressures to secure code training to scanning false negatives, developers have their backs to the wall when it comes to developing and releasing applications that not only perform the function they are asked to perform, but also do so in a way that protects the company’s prized data.

Identifying vulnerabilities is an important part of the process, but nothing is actually solved without remediation actions. Prevoty’s research shows that remediation is a headache for developers -- significantly impeding their ability to release applications on time and on budget.

Moving beyond best practices for building code, if developers and their managers want to reduce their exposure to risk, they need to find scalable ways to ensure application security and consider technologies that will help reduce the pain and drain of remediation.

METHODOLOGY

Prevoty surveyed more than 200 application and software developers in June 2015 through an online survey. Responses were collected from both male and female respondents, ages 18 and up, in the United States. Responses were voluntary and anonymous.