APPLICATION SECURITY: INTEGRATING DYNAMIC DEFENSE INTO SOFTWARE DEVELOPMENT
INTRODUCTION

In 2016, web applications represented only 8 percent of reported security incidents but 40 percent of successful breaches—up from just 7 percent of data losses the year before. That statistic points to the growing need to rethink application security, which often has been viewed as a compliance afterthought, development bottleneck or both. As federal agencies seek to modernize, develop and deploy applications more quickly, current approaches to application security can incur too much cost, delay and risk. How can agencies evolve their approach to application development to deliver as fast as the mission requires while avoiding vulnerabilities and costly remediation? In this paper, Accenture Federal Services provides an overview of modern application security and outlines an incremental way forward.

Talk with developers about application security and some themes are likely to emerge. Most will point out the immense pressure they face to deliver end products quickly. As they work to drive speed and innovation across web and mobile applications, security can seem more nuisance than necessity. In fact, many view it as a dreaded chore that they put off and strive to complete with minimal effort. While understandable, this viewpoint is increasingly risky given today’s application and threat landscapes.

THEN: DELIVER WORKING CODE

Historically, application security has been a discrete effort at the tail end of the development process. Many teams have tackled it as part of the testing phase with a goal of creating barriers to guard against unauthorized access to applications, systems and data.

Why is that approach becoming so dangerous? For starters, the application landscape is changing dramatically and rapidly as single-channel, static applications give way to dynamic, multichannel digital services. Increasingly, systems are composed of services from a variety of sources—legacy applications, Software-as-a-Service and digital platforms—and deployed via the cloud across numerous application channels, including mobile devices and embedded systems. At the same time, the notion of versioning has changed, as we no longer consume a specific service. Instead, we consume the current build, which may be replaced by a new one tomorrow. In other words, it is increasingly difficult to safeguard highly dynamic systems using static security reviews.

Furthermore, vulnerabilities may not be uncovered until very late in development, leading to risk of delayed launch and potentially high remediation costs. So, as web, mobile and other applications change more quickly—and become more integral to an agency’s operations—application security needs to evolve to keep pace.

NOW: DELIVER SECURE WORKING CODE

Security is no longer a vertical capability within an IT organization. Enabled by the increasing adoption of agile software development, security is rapidly becoming a horizontal mindset and skillset that must be applied during each sprint and across every aspect of development and operations.

In this context, one of the key objectives of agile—to rapidly deliver working code—must emphasize the delivery of secure working code as the ultimate goal. This requires that every developer has a security mindset, understands best practices and is enabled with the capability to apply those practices as part of day-to-day development activities.
THE CASE FOR DevSecOps

DevSecOps is increasingly being viewed as a model for integrating these disparate disciplines into a more holistic approach. Over the past several years, DevOps has established itself as a popular and effective way to bridge the gap between developing and operationalizing applications.

As DevOps continues to mature, organizations can adopt DevSecOps to more formally infuse security throughout application development, operations and maintenance. In the recent Accenture Federal Services white paper, Defining a Cyber Moonshot, DevSecOps was identified as one of five key steps agencies should pursue to improve cyber resiliency.

Pragmatically, DevSecOps addresses two enterprise objectives. The first is establishing, maintaining and enforcing a continuous loop of ever-evolving best practices for secure development and operations. The second: integrating security experts into the development process to better understand the steps being taken to safeguard applications and participate directly in trade-off decisions. In essence, it forward deploys the security audit process—accelerating launch by closing the loop between secure development and security validation.

As such, it can help federal agencies shift away from thinking about and investing in application development (including IT modernization) and cyber security as two separate initiatives. They can and, indeed, should be weaving development, modernization and security together as a single integrated focus with joint decision making.

DevSecOps helps to ensure that developers no longer assume security is not their job; it must be part of every iteration, every sprint and every time code is checked back in. Meanwhile, business stakeholders cannot pretend that security is not their problem. DevSecOps continually reinforces that they are the ones who pay the price when an application is breached.

There are even implications to how IT initiatives are funded. Within an agile project, teams always have a running list of desired new functionality, software enhancements and bug fixes. With security as a first-class stakeholder, the same should hold true of desired security features and capabilities. Security to-dos should be integrated with the other wish-list items and prioritized based on their ability to avoid costly issues. Creating a single funding model with a common backlog and joint decision-making helps ensure that security receives adequate attention among both product management, development and operations personnel. And, it improves an organization’s ability to balance the need for business features with the need for effective security.

While DevOps is an enabler that brings automation, repeatability, agility and speed across the entire lifecycle, DevSecOps transforms security into another enabler for the business. Whether or not an organization decides to embrace DevSecOps, every agency can benefit from a close examination of current application security practices. What follows is an overview of three levels of application security maturity—and indicators of progress against these goals.

A BRIEF WORD ABOUT DATA

While the focus of this paper is application security, we would be remiss not to mention a critical and complementary focus: data security. Strategies for hardening data—including access control and data classification, protection (masking, tokenization and encryption) and Data Loss Prevention (DLP)—will impact application security requirements. These strategies will be explored in a future paper.
GETTING STARTED: **THE GOOD**

Building and maintaining secure applications requires a focus on function as well as security. To balance business needs with security risks, start by focusing on these key areas:

1. **SET AND ENABLE STANDARDS.** A secure technical architecture integrated within the overarching business and security architecture is a critical first step to effective application security. An agency needs clear enterprise standards for secure development and application operations. Such standards need not be homegrown; taking advantage of industry standards, such as Open Web Application Security Project (OWASP), can help accelerate the process of codifying and adopting appropriate practices. Agencies also need to identify the necessary training and tooling that enables developers to effectively implement these standards in clear ways that can be validated in DevSecOps pipelines.

2. **MODEL THREATS TO ASSESS RISK.** A standard technical architecture is critical to security, but so is an understanding of the context in which an application will be used and the infrastructure in which the application will operate. Threat modeling considers that context to help in assessing the likelihood that a system will be a target and developing appropriate safeguards. Threat models can further assist in the development of security testing approaches that can be included in automated testing scenarios.

3. **USE TESTING TO IDENTIFY VULNERABILITIES.** Testing remains a key enabler of application security. Instead of saving it for the very end of the software development lifecycle, make it part of every development sprint. Static code analysis (SCA) uses basic testing to identify and flag areas with common mistakes. Complement that with static application security testing (SAST, or “white box testing”) to see if the application can be penetrated, as well as dynamic application security testing (DAST) to evaluate security when an application is running.

MAKING PROGRESS: **THE BETTER**

No application operates in a static environment, and each change can introduce new risks and vulnerabilities. Thus, the next critical milestone is staying on top of application security in a fast-evolving landscape. Penetration testing and vulnerability scanning should not be quarterly or even monthly activities. Adopt a proactive security posture and conduct such testing continuously as part of “business as usual.”

Beyond continual use of existing methods, federal agencies are well advised to explore newer techniques, such as application shielding and wrapping or application vaulting:

**SHIELDING AND WRAPPING** makes it possible to “cover” an application with additional layers of security—a capability that can be important in environments with citizen-facing web-based applications. It provides a vital layer of protection between the web front end and the systems and data that power it.

**VAULTING** involves placing the actual application in secured and encrypted storage. Users access its functionality through a continually reimaged version of the application—not the application itself. Vaulting keeps the original code under proverbial lock and key, safe from potential harm. It is a precursor to where application security is headed in the not-so-distant future (more on that in a bit).

These more advanced strategies become both more critical and more viable as agencies continue to integrate the cloud into their application architecture. While cloud-ready code is suitable for hosting in the public cloud, it may be limited in how it can take advantage of these more advanced security capabilities. By contrast, cloud-native applications are engineered for inherent cloud features that improve resiliency, security and failover.
STAYING SAFE: THE BEST

Today, the pinnacle of application security involves use of analytics to monitor the behavior of the application and its users. Application behavioral analytics empowers an agency with proactive insights into current and potential issues. Those insights are valuable in verifying and prioritizing remediation needs.

Beyond analytics, the “best” application security taps into a number of leading-edge capabilities. Chief among them:

RUNTIME APPLICATION SELF PROTECTION (RASP). Continual vulnerability assessment and penetration testing are important, but RASP takes proactive security one step further. Embedded within an application, this capability continuously monitors for and protects against suspicious activities. It does not merely flag potential issues; it takes action, such as terminating a user’s session or blocking execution of a function.

BUG BOUNTIES. People can be one of the greatest threats to application security. They can also be one of the biggest aids in shoring up security. By engaging the public through “bug bounty” programs, federal agencies can increase the likelihood of identifying and addressing a greater quantity of vulnerabilities in any application.

WHAT’S NEXT?

When it comes to application security, agencies today face a host of challenges as well as several opportunities to evolve their approaches. What might the future bring? While no one has a crystal ball, there are a number of trends that are gaining momentum and are worth considering as part of an enterprise strategy for secure application development.

Two major forces—living applications coming of age and cloud going mainstream—are poised to disrupt the application security landscape. This requires federal agencies to continue to consider new approaches to stay secure. Among them:

CLOUD ACCESS SECURITY BROKERS (CASBS). These are security policy enforcement points that live on premises or in the cloud and serve as a barrier between cloud service providers and consumers. CASBs can play a key role in addressing risks, enforcing policies and complying with regulations even when applications and data are outside an agency’s immediate control.

POLYMORPHIC CODE. In the future, cloud itself will evolve into a security feature—and polymorphic code is one of the most promising ways. As the name implies, polymorphic code continually changes forms. Developers may craft ten to 15 versions of the same code and place them all in the vault. The system then randomly pulls one set of code from the vault, where the “real work” is done, and brings that to the application surface. In essence, polymorphic code fights hackers with a dose of their own medicine. It makes an attack surface so dynamic that it never looks the same and therefore becomes much more difficult to understand and penetrate.

CONCLUSION

As with any resource, applications are most secure when they control choice. That starts from design and development and continues through deployment and day-to-day use. By tightly integrating security into application development and maintenance, DevSecOps helps ensure that addressing security is not an option or an afterthought. And by leveraging some or all of the latest techniques and technologies, applications can help close any gaps that leave them vulnerable to breaches. While the journey from “working code” to “secure working code” does not occur overnight, prudent agencies are not delaying in taking the initial steps—including articulating an application security strategy.
REFERENCES

1 Synopsis: https://www.verizondigitalmedia.com/blog/2016/06/verizon-dbir-2016-web-application-attacks-are-the-1-source-of-data-breaches/


ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 425,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

ABOUT ACCENTURE FEDERAL SERVICES

Accenture Federal Services is a wholly owned subsidiary of Accenture LLP, a U.S. company, with offices in Arlington, Virginia. Accenture’s federal business has served every cabinet-level department and 30 of the largest federal organizations. Accenture Federal Services transforms bold ideas into breakthrough outcomes for clients at defense, intelligence, public safety, civilian and military health organizations. Visit us at www.accenturefederal.com.