The primary attack vector: applications

Reduce risk and cost by designing in security

January 14, 2019

perspecta™

Is it time to reprioritize?

As cybersecurity threats become more mature, more focused and more dangerous, companies and governments throughout the nation and around the world continue to struggle to provide an acceptable level of protection for their intellectual and physical property and the data they safeguard.

How much security is enough? This question plagues governments and businesses alike; clearly, there is no one right answer. Any breach resulting in exposure or loss of critical information is one too many. Network/perimeter security was the initial frontier for cybersecurity professionals. By and large, the level of protection that has been accomplished in this area has effectively prevented most attempts at breaching the foundational layer of the cybersecurity protocol stack. Today, that is not enough. It is no longer practical to disallow almost all communications through the network layer. The attacker looks for the weak underbelly of IT, and that is where we need to look as well.

In the *2018 Application Security Report*, cybersecurity insiders indicate that less than half of organizations implement security architecture and design, with under a quarter performing threat modeling.[1] Positive Technologies report that in 2017 "almost half of web application [were] vulnerable to unauthorized access."[2] And, according to *The 2018 Hacker Report*, websites are the favorite attack point for more than 70% of hackers.[3] As identified in the *2018 Data Breach Investigations Report*, the largest number of breaches, about 1 in 5, are directly associated with web applications.[4]

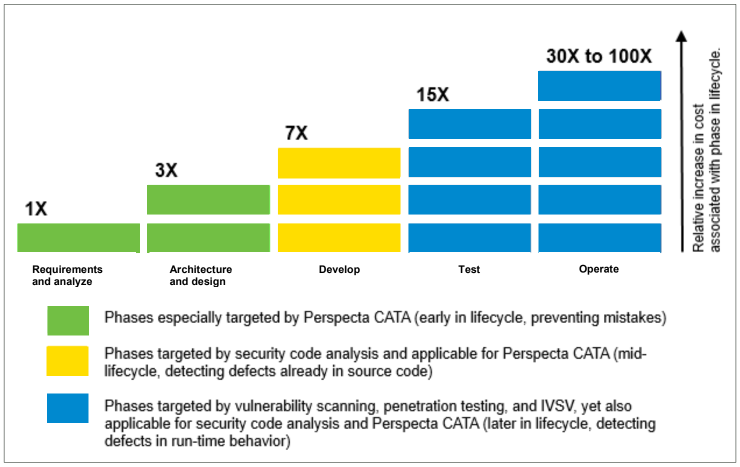
Understanding and responding to the most common threat vector is the right start to implementing a more effective cybersecurity prioritization process. The applications layer has been largely under-protected and it is now vital to strengthen our cybersecurity posture in this area. While organizations have to be vigilant at every layer, application security should be the "new normal" and at the forefront of every organization's cybersecurity defenses. Now is the time to take a proactive approach by protecting the adversary's biggest target—applications.

Build in; Don't bolt on

It is a well-established fact in software development that the earlier a defect is avoided, or discovered and removed, the more cost can be contained or reduced.

Various studies have shown that software defects found and fixed after deployment will cost an order of magnitude more than if they had been found (or avoided) at the beginning of the life cycle. The National Institute of Standards and Technology (NIST) estimates it is 30 times or more expensive to "bolt on" quality after deployment.[5] Barry Boehm, the inventor of the Spiral Lifecycle[6] and who was also quoted in the NIST study, found a 100 times increase in cost when defect discovery and repair was delayed.

The following graphic illustrates the relationship between the phase in which the remediation occurs and the cost of the remediation.



[1] Cybersecurity Insiders, *2018 Application Security Report*, p. 16.
[2] Positive Technologies, *Web Application Vulnerabilities: Statistics for 2017*, p. 4.
[3] HackerOne, *The 2018 Hacker Report*, p. 22.
[4] Verizon, *2018 Data Breach Investigations Report*, 11th ed., p. 22.
[5] NIST, *Planning Report 02-3: The Economic Impacts of Inadequate Infrastructure for Software Testing*, NIST Acquisition and Assistance Division, Gaitherson, MD, USA, RTI Project Number 7007.011, May 2002.
[6] B.W. Boehm and P.N. Papaccio, "Understanding and controlling software costs," *IEEE Transactions of Software Engineering*, vol.14, no. 10, Oct., pp. 1462-1477, 1988.

The cost of reactivity

To put it plainly, quality is a “pay a little now…or pay a lot later” challenge, but “later” can mean almost immediately in application testing or deployment. Delaying defect repair will increase exposure, risk and costs. When the quality you are assessing is actually a cybersecurity risk, the stakes get very high. You can roll the dice and hope that your application won’t be compromised, but you must be prepared for the cost of the breach, which would typically represent an order of magnitude or more above what it would cost to find and fix the problem in the development stage.

Vigilance is more important than ever. Vulnerabilities, or security defects, are deficiencies that allow attackers to perform unauthorized actions and circumvent protection mechanisms. The cost of these vulnerabilities can have serious financial and operational ramifications, risking mission success or business function, data loss, or delaying deployment. Once applications are in production, undiscovered vulnerabilities increase risk and costs even more, requiring expensive software testing, updates and patching.

Though application cybersecurity has long been a legislative priority, it remains a national issue, as evidenced by the “Cybersecurity and Infrastructure Security Agency Act of 2018,” which includes requirements for:

- “comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure”[7]

The updated DODI 5000.02, Operation of the Defense Acquisition System 2017, adds a dedicated cybersecurity chapter, requiring cybersecurity to be fully considered and implemented in all aspects of acquisition programs across the life cycle.[8] It includes early life cycle activities such as:

- Understand Cybersecurity Requirements
- Characterize Cyber Attack Surface

Most assessment methodologies assume defects are, or can be, discovered through normal testing procedures. However, application testing tends to focus on functionality and some known vulnerability types, which can leave applications vulnerable to previously unknown vulnerability types. The result is that security defects are discovered only after a breach has occurred.

The severity and frequency of attacks today requires ever-increasing expenditures for remediation. The smart move is to review current security practices employed during application development to ensure a “built-in security” approach versus the traditional “bolt-on” security approach is followed. Designing and building a robust security architecture can both prevent defects and reduce the impact of other defects, which can either reduce or eliminate the impact of defects in an application. The “built-in security” approach can actually reduce the total cost of development and operation of an application as well as provide enhanced, up-front protection against latent vulnerabilities.

The proactive approach

Perspecta focuses on proactively improving security at every stage of the software (or systems) development lifecycle (SDLC). This means “architecting security in” from the beginning, with a laser focus on applications specifically within the architectural layer to avoid tens, hundreds and sometimes thousands of vulnerabilities at a time. Often with a single architectural change or applying secure design principles, many vulnerabilities are eliminated or mitigated. This both improves security and reduces cost. Specifically, the Perspecta comprehensive applications threat analysis (CATA) service can ensure cybersecurity is built in.

The CATA service helps our customers identify critical yet missing security requirements in application development as well as those architectural choices that unnecessarily—and often dramatically—increase the number and severity of both known and unknown vulnerabilities. Using CATA, specific recommended actions are identified to address problems from both a regulatory perspective and an architectural threat model view.

This service highlights activities in the earliest phases of the development life cycle, the requirements and architecture/design phase, but is

[7] Cybersecurity and Infrastructure Security Agency Act of 2018, H.R. 3359 (2018).

[8] DODI, Operation of the Defense Acquisition System, No. 5000.02. 7 Jan. 2015. Updated 10 Aug. 2017.

also used to validate security resiliency for applications already in production.

Examining the requirements and security architecture of existing applications provides an identification of security risks, allowing a fact-based, comprehensive approach to address security risk in an application instead of piecemeal patching efforts as individual security defects are detected. While not as optimal as including security in the initial design, proactively addressing existing risks remains more cost effective than waiting for the security defects to be discovered and a breach to occur.

CATA differs from industry-standard applications security methodologies by attacking the problem from a requirements and architectural viewpoint, which helps eliminate entire classes of vulnerabilities rather than just individual weaknesses, which takes excessive time and effort to remediate.

The best way to secure applications is to think about cybersecurity early on as well as throughout the development life cycle. Consider the following comparison of applications security methodologies: a large commercial software vendor developed two versions of an application, one to support Linux/UNIX and another for Windows. The UNIX application utilized CATA while the Windows version used traditional development approaches. The CATA process assessed and enabled the resolution of security requirements gaps and architectural security resiliency early in the process. The application that used CATA avoided more than 70 vulnerabilities as a result of addressing a single finding, while the other methodology resulted in multiple patches and security bulletins to react to the same vulnerabilities after deployment. As previously mentioned, CATA findings can often avoid tens, hundreds and sometimes thousands of vulnerabilities. The small, up-front investment in security quality improvement can pay for itself many times over in avoiding expensive, reactive security fixes and patching.

CATA gives you a strong security foundation

Review	Development	Release	Results
No review	Security defects unknowingly introduced during development	70+ security defects needed to be fixed in post release security advisories creating high risk and high remediation costs.	Higher risk and cost
Perspecta CATA review	Review during development phase avoided 70+ vulnerabilities.	Security defects fixed before release, reducing post-release risk and patch costs.	Reduced risk and cost

The optimized approach

Developing a fully optimized cybersecurity approach requires a holistic viewpoint of an application’s security balanced with complementary processes and tools. By designing security in and then augmenting with conventional application security approaches, all phases of the SDLC can be addressed and maintenance costs are reduced while increasing security.

This optimized approach combines secure architectural design principles, security code analysis or scanning, vulnerability assessments and penetration testing to avoid, mitigate, find, or fix vulnerabilities as early as practical, resulting in fewer vulnerabilities to be addressed at the most expensive time—late in the development life cycle.

In a world of ever-shrinking budgets, increasing IT efficiency is one of the few ways you can cut costs. By utilizing a secure application development approach, the total cost of development/operation is reduced. This is an ideal way to cut costs while increasing security at the same time.

For more information

If you have an interest in ensuring your applications have security built-in from the ground up, the Perspecta cybersecurity CATA team can work with you on a proof-of-concept or a full engagement to help you mature your security architecture and profile.

Learn more at:

perspecta.com/offerings/cybersecurity