IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

The Benefits of Continuous Testing

Tamar Everson

Tamar Everson
Lead Security Consultant
Context Information Security

Biography

Tamar Everson is Lead Security Consultant at IT security specialists, Context Information Security (https://www.contextis.com).

He started his digital security career in 2012 by joining Glasgow Caledonian University's digital security programme and established the GCU Ethical Hacking Society in 2014, helping members attend conferences across Europe, hosting guest speakers and workshops, as well as holding the NASA International Space Apps Challenge.

Tamar blogs at https://www.contextis.com/en/blog

Keywords Testing by design, Cybersecurity, DevSecOps, Agile, Continuous testing
Paper type Opinion

Abstract

Organizations often invest considerable time and effort into transforming their development processes to meet business demand, yet their testing processes remain stuck in the past. In this article the author looks at the value of security testing early and often. Defined as a software testing methodology, continuous testing involves a process of testing early, often and everywhere, and needs to be on the agenda for every organization.

Introduction

The traditional approach to security when developing a new software application, IT product or system has been to build it, test it and wait for something to go wrong. But this reactive find and fix approach is a costly, time consuming and risky way of doing things. Instead, companies are now looking to benefit from having security assurances much earlier in the project lifecycle, with security being implemented 'by design' and throughout the lifecycle of the project.

The value of what we call Continuous Security Testing reflects the trends of Agile development and DevSecOps, automating and integrating processes and related security measures from the very beginning of the development cycle. Testing early and testing often, results in better protection, quicker times to market, or deployment and reduced costs.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Identifying vulnerabilities

While a traditional penetration test is a snapshot-in-time assessment, continuous security testing allows vulnerabilities to be identified, remediated and retested throughout the development process – rather than applying costly post-development patches. Usually, security testing takes place at the end of each Agile 'sprint' which allows any identified issues to be added to the backlog and prioritized for fixing in the following sprints, before the cycle continues. This method is particularly useful for applications developed in short iteration cycles, because modern development methods often don't allow the time for manual tests.

Continuous security testing is efficient at finding a wide array of vulnerabilities including injection attacks, Cross-Site Scripting (XSS), and session-related issues. While they are the same ones we typically find in other types of engagements, being able to implement fixes before a project goes live removes the need for separate teams having to make fixes at a later date. Working with the same team also helps to get a more in-depth understanding of the application, development process and the business decisions behind the system's design, which means that findings can be better targeted to the needs and concerns of customers. Being embedded with the development team also breaks down the traditional barriers between developers and security testers.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Reporting is generally done straight into bug tracking software, which allows developers to gain immediate, easy-to-digest visibility so that they can prioritize accordingly. From a security tester's perspective, you can find an issue, inform the development team and have it fixed and re-tested within the hour.

While automated vulnerability scanning tools can be used to provide a similar type of frequent assurance on the security of your internet-facing systems, it is worth noting that they are not very effective at finding business logic-based issues and can be prone to false positives. Continuous security testing follows a manual penetration testing methodology and will always provide greater depth than an automated scan. In the end, automated tools are only as good as their libraries, so if they aren't updated often they won't be able to detect the latest attacks.

In conclusion

The rush to market can often compromise security, but this is no longer an option. Security by design is now the mantra for the technology industry. But this has to go hand in hand with early and continuous security testing to ensure the integrity of a new application, product, or system through its entire lifecycle – achieved by harnessing the best manual skills and automated tools.