Application security crucial for data protection

By Simeon Tassev

18 Dec 2015

Software is often considered the cornerstone, supporting essential business processes, enabling productivity and facilitating enhanced efficiency, to name but a few functions. Catering to trends such as mobility and always-on connectivity, applications are now more accessible than ever before, and are available through a wide variety of platforms, including the web, cloud, and mobile devices.

©bloomua via 123RF

The challenge lies in the fact that, in order to perform their primary functions, software applications require access to data - the currency of the modern enterprise. The more open, connected and available applications become, the more they extend beyond the traditional boundaries of the organisation. This often puts them outside the control of security defences, potentially leaving sensitive information vulnerable to a variety of threats. Application security is therefore an essential component of an effective overall data protection strategy, particularly when dealing with confidential customer information.

Security strategy

Applications are typically not built with security in mind, focusing on delivering functionality. As a result, they are often an overlooked aspect of security strategy. However, without effective application security, these very tools could expose sensitive information, leaving it unprotected and vulnerable. Cyber crime has become big business, and with such vulnerabilities open to exploitation, organisations are increasingly at risk of a variety of threats. This includes theft of data, customer information and intellectual property, disruption of business operations, damage to brand and reputation, and opening up employees and customers to risk, including the risk of identity and payment information theft.

Application security is particularly critical for organisations dealing with online commerce and trading. These organisations need to effectively secure not only confidential customer information, but comply with regulations around securing payment card information as well. The nature of the threat is evident when one examines a number of recent website data breaches, including the recent case of United Airlines. The company admitted to three dozen of its MileagePlus loyalty card accounts being compromised as part of an attack that reused login credentials obtained from a third party source. The reality is that this type of crime is inevitably on the rise, as perpetrators of hacks often sell the data they steal, making this type of crime highly profitable.

Proof in the numbers

Some statistics highlight the magnitude of the problem. According to the Symantec Internet Security Threat Report of April 2015, the retail industry "liable for the largest number of identities exposed, accounting for almost 60% of all identities reported exposed" and the number of breaches containing financial information amounted to 35.5%, most frequently credit or debit card details. A significant proportion of this information was obtained via online channels. In addition, according to the report, "real names, government ID numbers, and home addresses were the top three types of information breached in 2014". This information is all confidential to the customer, and represents a breach of the Protection of Personal Information (PoPI) Act in South Africa.

Further to the challenge of securing payment information within web applications, organisations also need to ensure the mobile dimension is addressed. According to the Symantec report, "there are now more than 1 million malicious apps in existence; proof-of-concept attacks on the Internet of Things are here, including wearables, internet infrastructure, and even cars; and devices on the cusp of the Internet of Things, such as routers, network-attached storage devices, and embedded Linux devices, are already under attack." Mobility effectively creates additional loopholes for criminals to exploit when launching attacks aimed at data breaches.

The recently published 2015 "HP Security Research Cyber Risk Report" highlighted that 80% of mobile applications unintentionally reveal potential benefits to malicious hackers while 71% store data in an unsecure manner, 65% do not protect data via encrypted communication or other means and 31% can reveal geolocation. In addition, this report highlights that fundamental application security errors in coding still occur and Appsec vulnerability also exists outside the application code. For example, 52% of web applications experience issue with input validation, including cross-site scripting, SQL injection and other vulnerabilities. Furthermore, 82% of these web applications with vulnerabilities related to server misconfiguration, improper file settings and outdated software to mention a few.

As these facts and figures illustrate, application security is essential. It is also however an issue that is the subject of much debate on how to effectively achieve. While there is much discussion on the most effective approach to application security, consensus is that it is essential to start with security built into the software development lifecycle. If security is built into the framework and process of the actual application development, it will prove far easier to enforce on a granular level.

Mitigating risk

However, actually achieving this goal is all but impossible for the majority of organisations, as they often need to make use of existing systems and legacy solutions that must integrate with each other, inherently opening up vulnerabilities. Mitigating this risk requires appropriate tools for access control, data protection and more. In addition, it is essential to incorporate application security and testing into security strategy, including vulnerability testing of the underlying application operating system and all related dependencies. In addition, specific application testing, including web and mobile security, should be included, as well as code scanning solutions to examine the actual application code for vulnerabilities.

When it comes to protecting information, and especially confidential customer information such as payment data, adherence to regulatory legislation such as the Payment Card Industry (PCI) Data Security Standard (DSS) is enormously beneficial. PCI DSS represents the minimum best practice standards required for data security, including specifications for

application security, along with policies, procedures and more. PCI as a best practice can be applied in many organisations, whether they process payment information or not, and can go a long way toward mitigating the risk of application vulnerabilities and related data breaches in organisations.

ABOUT SIMEON TASSEV

Simeon Tassev is the director of Galix, a reseller of Mimecast Solutions in South Africa
- Cybersecurity awareness is no longer a generic exercise for business - 7 Feb 2023
- Understanding cybercrime's true impact is crucial to security in 2021 - 3 Feb 2021
- What can we do to stop ransomware attacks on governments? - 16 Dec 2019
- Cyber security professionals are no Darth Vader - 19 Mar 2019
- How to create a cybersecurity culture - 16 Jan 2019

View my profile and articles...