CYBALT

Why is Application Security Important for Business?

Why is Application Security Important for Business?

A Growing Risk

In today's world of ever growing digitization, application security is getting a lot of attention.

The rapid growth in the application security segment has been accelerated by the changing way enterprise apps have been constructed in the last several years. Gone are the days where an IT shop would take months to refine requirements, build, and test prototypes, and deliver a finished product to an end-user department. The idea almost seems quaint nowadays.

While applications are core components of a business relying on technology (and that's almost every business), underlying security threats remain a point of significant concern. Modern applications are highly distributed and most of them are connected to the cloud. This further increases the attack surface available for malicious actors.

With the rising adoption of software applications in business, an increase in cybersecurity attacks shows a corresponding upward trend. To tackle such attacks, an efficient application security (AppSec) mechanism requires a combination of tools and practices for identifying, remediating, and preventing security vulnerabilities throughout the application development life cycle. By proactively fixing vulnerabilities, security teams improve the application's security posture since threats are mitigated before being exploited in production.

The Tools of the Trade

Hundreds of tools are available to secure various elements of your applications portfolio from locking down coding changes to assessing inadvertent coding threats, and evaluating encryption options to auditing permissions and access rights. There are specialized tools for mobile apps, for network-based apps, and for firewalls designed especially for web applications.

This is a process of making your applications more secure by finding, fixing, and enhancing the security of applications. Application security in itself is a broad subject that requires multiple practices and tools to work in sync.

Much of the security work happens during the application development phase. But security work continues and includes tools and methods to protect apps once they are deployed. This is becoming more important as hackers are increasingly targeting applications.

Time is of the Essence (or Sooner Rather than Later)

The faster and sooner in the software development process you can find and fix security issues, the safer your enterprise will be. Because everyone makes mistakes, the challenge is to find mistakes in a timely fashion. For example, a common coding error could allow unverified inputs. This mistake can turn into SQL injection attacks and lead to data leaks if a hacker finds them.

Application security tools that integrate into your application development environment can make the process and workflow simpler and more effective. These tools are also useful if you are doing compliance audits, since they can catch problems before the auditors catch them saving you the time, expense, and hassle of fixing them later.

The Business Value of an Application Security Strategy

Application security in itself is a broad subject that requires multiple practices and tools to work in sync. An entire application security strategy encompasses several steps and can be categorized into different types depending on the features covered. These include authentication, authorization, encryption, logging, and testing.

Modern software development primarily emphasizes agility, where most of the efforts are concentrated on streamlining the continuous integration/continuous delivery (CI/CD) pipeline. AppSec, on the other hand, blends security seamlessly into development and operations workflows to build safe applications while keeping development costs low.

Data security and privacy are core aspects of every application security approach. Every application processes and stores sensitive business information and customer data, often the prime targets in a breach. A data breach leads to loss of confidence and trust of valuable customers and tarnishes business reputation in the longer run. On the contrary, administering appropriate AppSec mechanisms and data privacy policies also helps boost brand value since consumers associate with businesses that comply with robust data security safeguards.

Most users are concerned by how systems handle their data. With proper data privacy regulations in place, customers are guaranteed safety against identity theft and credit card fraud and thus trust the platform. Adopting data protection policies also enforces an effective ethics code since handling data responsibly is considered general ethical practice. Failure to protect sensitive customer data also results in penalties from regulatory authorities leading to loss of revenue or operating licenses.

With more workloads moving to the cloud, it is vital to choose a cloud service provider whose platform includes reliable security solutions and is compliant with regulatory standards to prevent data misuse. Apart from choosing the right service provider, it is common to use tools that form the first line of primary defense. These include application firewalls, role-based access control (RBAC), multi-factor authentication, and input validation for incoming traffic. As a recommended practice, cloud service providers require the use of service tags to enable fine-grained control for network access.

Depending on the stage in the software development life cycle (SDLC), there are different approaches to ensuring application and network security. Some standard methods include design review, code review, black-box testing, Coordinated vulnerability management, and automated testing (Static Application Security Testing [SAST)] dynamic application security testing [DAST], software composition analysis (SCA), and runtime application self-protection (RASP).

Sustainable Security

As we continue to live with more and more digitization, an era where our private data is shared across applications, security is the key part of modern-day applications. A small vulnerability can be exploited and result in major data leaks invading user privacy. This data can be used to further exploit the user's finances. Hence it is key that application security be taken up as a highest priority and you have a sustainable solution in place to meet and accommodate its dynamic nature.