TATA CONSULTANCY SERVICES

Building on belief

Low-code platforms

An exploration of the security threats and mitigation strategies

Abstract

The confluence of advanced automation technologies, the rise of cloud computing and the digitalization of business processes, all exacerbated by COVID-19, and the need to support remote working capabilities, has accelerated the use of low-code platforms. A report by Gartner states that by 2023, over 50% of medium to large enterprises will have adopted low-code platforms as a strategic application platform[1]. Besides accelerating the development of new applications, these platforms also empower non-technical users to create apps.

On the flipside, low-code platforms create new security vulnerabilities. Moreover, the processes and controls around these platforms are still nascent. Hence, organizations bear the onus of mitigating the threats and ensuing exposure from these applications by employing stronger governance and compliance policies. This paper examines the security threats of ungoverned low-code platforms and the approaches to reduce those risks.

The threats inherent in low-code platforms

It is a given that data security is of utmost priority for organizations to protect their data from vulnerabilities to external threats such as ransomware, malware, phishing, DDoS attacks, and more. However, low-code platforms can be used by anybody in an organization, giving leeway to internal threats – be it from unintentional mistakes by the user or mala fide intent. Hence, it is imperative that effective security solutions are built into applications to protect data from internal breaches.

Figure 1 showcases how a typical citizen developer fulfills their app development requirements, and how organizations introduce the governance (security and compliance) layer.

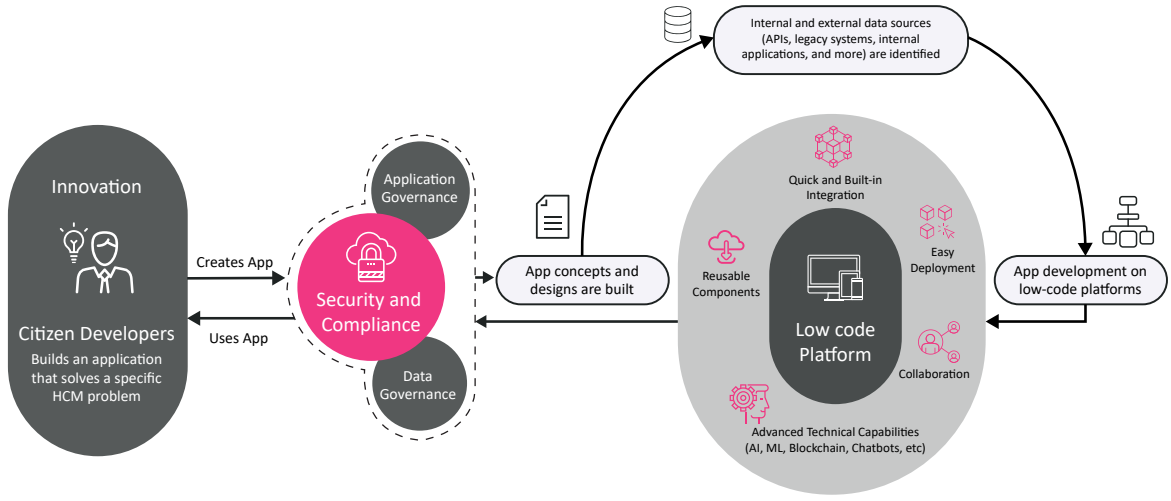

Figure 1: App development on low-code platforms

[1] *Gartner; Gartner Magic Quadrant for Enterprise Low-Code Application Platforms; August 8, 2019; https://www.gartner.com/en/documents/3956079/magic-quadrant-for-enterprise-low-code-application-platf*

Most leading low-code platforms have a standard set of security and compliance requirements implemented at the platform level itself. While these platforms include global, US-specific, industry, and regional compliance offerings, organization-specific compliances or security measures still need to be implemented at the individual company level. Ungoverned low-code platforms could be the biggest threat for any kind of organizational security or compliance breach, as they are extensively used by all business users.

Web or mobile applications built on low-code platforms are not inherently secured. Though security and compliance controls are implemented at the platform level, some of these measures are required at the application level as well.

Areas of security vulnerabilities

Applications built on low-code platforms are as vulnerable to security threats as other applications. Enterprises need to assess both internal and external risks and threats and must have strategies to safeguard their applications built on low-code platforms. Figure 2 illustrates the various areas where applications can become vulnerable to security risks.

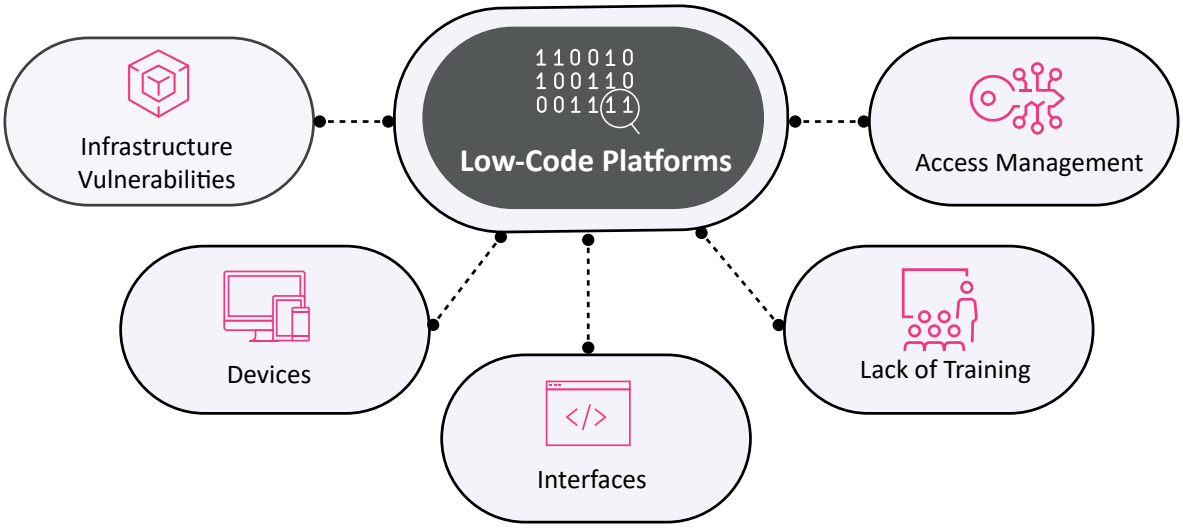

Figure 2: Vulnerabilities on low-code platforms

Infrastructure vulnerabilities

These kinds of vulnerabilities are a major threat to the core of a system, impacting application security. Examples of infrastructure vulnerability are weak firewall designs or assumptions, TCP/IP vulnerabilities, insecure wireless access points, and inadequate operating systems.

Such vulnerabilities are largely addressed at the design stage and mitigated at the platform level. Nonetheless, vendors should focus on how to efficiently and effectively address customers' customized requirements and individual challenges.

Flawed access management

Due to inherent flaws in access management, most application security is compromised at the user, data, or application programming interface (API) access level. However, properly designed access to data, APIs, or users can help enterprises address most application security threats, including those built using low-code platforms. Though these apps leverage reusable components or templates, user and data access management details within the applications are often neglected.

Lack of security training for citizen developers

The ease of application development with low-code platforms has encouraged more and more business users to develop in-house applications. While this reduces costs, the downside is that most business users are not trained application developers. In fact, it is likely that they may compromise on security threats while developing the applications, thereby making applications developed on low-code platforms vulnerable.

Interfaces with APIs

The ability to quickly integrate or interface any APIs, third-party applications, or legacy applications will expose the app to the security threats associated with those interfaces. The APIs, third-party applications, or components which are integrated may or may not be fully authorized or tested. A report by cybersecurity firm Salt Security states that 27% of organizations do not have any security strategy in place for APIs[2].

Insecure personal devices

COVID-19 has ushered in telecommuting, where most work is executed online. Most employees prefer using their personal devices such as their mobiles or tablets for official assignments. Since these personal devices are not monitored, viruses or hidden malicious applications leave ample room for attacks and data leakage.

Approaches to mitigating security threats

To mitigate these threats, an organization's strategy and mindset should focus on the challenges and opportunities offered by newer technologies. Despite their ease of development, cost effectiveness, and agility, developing applications through low-code platforms should be treated on par with any other application development.

The factors that can enhance system security are as follows:

DevSecOps

Most low-code platforms have tools which support DevOps. Although DevOps is already built into the application development cycle, it is imperative to also include security processes within DevOps. DevSecOps imbibes all the security processes or operations within the application development life cycle itself.

More than a process or operation, it is a cultural shift. DevSecOps is a mindset which gives due importance to security and integrates the processes or checks which are required to secure applications.

Application governance

On low-code platform apps, application governance, data governance, and governance on external or internal interfacing should be defined with configurable governance settings. This facilitates what data connectors are to be allowed and what needs to be restricted at the platform level itself. However, extra vigilance and caution need to be exercised while integrating external or open source APIs with an application. Extensive tests on such external interfaces can rule out potential security vulnerabilities.

---

[2] Help Net Security; API security concerns hindering new application rollouts; February 4, 2021; https://www.helpnetsecurity.com/2021/02/04/api-security-concerns-hindering-new-application-rollouts/

Application security training

Unless required, most citizen developers or business users are not trained coders. Therefore, it is imperative that they be trained and made aware of the security threats prevailing in application development. Implementing stringent security checks is a collective responsibility within an organization, across all levels.

Security testing tools

The main drawback of low-code platforms lies in their intrinsic architecture. Most security layers in low-code platforms are like black boxes. This makes manual testing and debugging by a developer or security tester virtually impossible. Furthermore, manual testing and debugging low-code applications will only affect the main advantage of such platforms - the speed of development and delivery and the time to market.

Enhancing security systems of cloud services

Low-code platforms are mostly built on public or private cloud services. While the security of private cloud services is considerably robust, this is not the case for public cloud services. To secure the public cloud, enterprises can leverage security services from platforms such as Microsoft Azure, Amazon Web Services, and Google Cloud. They can also help their teams use continuous integration and continuous delivery (CI/CD) pipeline tools. They enable continuous checks for security threats and risks, besides frequent and reliable incremental code changes.

The future of low-code

The rise of low-code development platforms is largely attributed to benefits such as reduced inefficiencies, quicker solution delivery, increased focus on data security, and decreased overhead costs.

As IT technologies rapidly evolve, low-code development platforms - which come with their own platform-level security and governance - might not provide solutions to every kind of emerging development challenge. Nonetheless, they have paved the way for simplification and enhanced speed-to-market across the software development value chain.

Implementing security and governance checks at both the enterprise and developer levels can help organizations reap the benefits of low-code platforms without compromising on security. These advantages can be realized with the right mindset and best practices, thereby allowing enterprises to create solutions for a purpose-driven, resilient, and adaptable future.

About the authors

Atul Jagnale

Atul Jagnale is the chief technology officer for the UK and Europe for HiTech at TCS. He is also a domain lead in the Digital and Enterprise Transformation unit. In his current role, he designs new sales plays with a focus on innovation and platform-led growth and transformation for existing customers and new prospects. Atul holds a master's degree in electronics and power from Visvesvaraya National Institute of Technology, Nagpur, Maharashtra, India.

Rinkal Brahmbhatt

Rinkal Brahmbhatt is a digital workplace and low-code platforms evangelist for HiTech at TCS. In her current role, she provides consultation and advisory services on digital workplace services and solutions to TCS' customers globally. She holds a master's degree in computer applications from AES Institute of Computer Studies, Ahmedabad, Gujarat, India.

Contact

Visit the HiTech page on www.tcs.com

Email: HiTech.Marketing@tcs.com

About Tata Consultancy Services Ltd (TCS)

Tata Consultancy Services is a purpose-led transformation partner to many of the world's largest businesses. For more than 50 years, it has been collaborating with clients and communities to build a greater future through innovation and collective knowledge. TCS offers an integrated portfolio of cognitive powered business, technology, and engineering services and solutions. The company's 469,000 consultants in 46 countries help empower individuals, enterprises, and societies to build on belief.

Visit **www.tcs.com** and follow TCS news **@TCS_News**.

Corporate Marketing | Design Services | M | 08 | 21