CxO Trust Newsletter - April 2022

C-Level Guidance to Securing Serverless Architectures

Hillary Baron, Director of Research, Analytics, CSA

As businesses work to bring technology value to market faster, serverless platforms are gaining adoption with developers as they provide a more effective way to move to cloud-native services without managing infrastructures such as container clusters or virtual machines. In response to serverless architecture's growing appeal, the paper examines the business benefits of serverless architectures — such as agility, cost, and speed to market — with a focus on serverless application security and industry-wide best practices and recommendations for implementation.

Despite the security challenges, when used properly, serverless capabilities can provide security benefits when compared to transitional applications, including stateless and ephemeral components, inherent data compartmentalization, and, in some cases, simplified patching.

Serverless computing offers several business benefits over traditional cloud-based or server-centric infrastructure, however, as with any emerging technology, serverless brings with it a variety of unique cyber risks. The evolution of any technology is inevitably followed by the evolution of threat actors looking to exploit its vulnerabilities. It's critical, therefore, that new technologies are adopted carefully and that proper diligence is undertaken.

The latest report from the Serverless Working Group provides a high-level business overview of Serverless architectures and examines three critical security areas for serverless applications, namely threats that stem from actions taken by:

1. application owners when setting up infrastructure to host an application
2. application owners during the process of deploying their applications
3. the entity providing the service and/or infrastructure to application owners