Reproduksi dan Penanganan Ancaman Internal dari Implementasi Zero Trust Architecture pada Kubernetes Menggunakan Service Mesh = Reproduction and Handling of Internal Threats from Zero Trust Architecture Implementation on Kubernetes Using Service Mesh

Fairuza Raryasdya Ayunda, author

Abstrak

Pengadopsian Kubernetes sebagai bagian dari sistem terdistribusi meningkatkan kompleksitas pengelolaan sistem sehingga dapat membuka peluang ancaman keamanan. Model keamanan Zero Trust pun dikembangkan untuk menangani masalah keamanan akibat peningkatan kompleksitas tersebut. Berfokus pada perlindungan resources, model keamanan ini membatasi kerusakan yang dapat ditimbulkan penyerang dengan memberikan akses terbatas ke setiap pengguna. Pada Kubernetes, penerapan Zero Trust Architecture dapat dibantu dengan memanfaatkan fitur-fitur keamanan milik service mesh. Namun, penerapan Zero Trust Architecture pada Kubernetes dengan menggunakan service mesh masih belum dapat menangani ancaman internal yang disebabkan oleh penyerang yang menyalahgunakan privileges-nya sebagai Cluster Administrator. Ancaman internal tersebut diidentifikasi dan kemudian direproduksi pada sistem acuan penelitian ini. Hasil reproduksi menunjukkan bahwa sistem acuan belum terlindungi dari ancaman internal. Oleh karena itu, penanganan terhadap ancaman internal tersebut dilakukan dengan mereproduksi sistem solusi berupa validasi signature terhadap konfigurasi manifest atas pembuatan dan modifikasi resources pada Kubernetes melalui admission controller. Sistem solusi kemudian diuji dengan dilakukannya reproduksi ancaman internal tersebut. Berdasarkan hasil pengujian, ancaman internal telah berhasil ditangani oleh sistem solusi.

.....

The adoption of Kubernetes as part of a distributed system increases the complexity of managing the system, which can lead to security threats. The Zero Trust security model was developed to address the security concerns resulting from this increased complexity. Focusing on resource protection, this security model limits the damage an attacker can cause by granting limited access to each user. In Kubernetes, implementing Zero Trust Architecture can be aided by utilizing the security features of service mesh. However, the implementation of Zero Trust Architecture on Kubernetes using service mesh is still unable to handle internal threats caused by attackers who abuse their privileges as Cluster Administrators. These internal threats are identified and then reproduced on the baseline system of this research. The reproduction results show that the baseline system is not yet protected from the internal threats. Therefore, the internal threats are addressed by reproducing the solution system in the form of signature validation of the manifest configuration for the creation and modification of resources on Kubernetes through the admission controller. The solution system is then tested by reproducing the internal threats. Based on the test results, the internal threats have been successfully handled by the solution system.