PRESS RELEASE

3 Factors for Enhancing Container Security

At it-sa 2019 msg shows what really matters when using container technologies and container orchestration – from a security point of view

Munich, September 12, 2019. Today, the idea of agile software development without DevOps is unimaginable. At the same time, the use of Dockers and other container technologies in DevOps scenarios is becoming much more common given all the advantages they offer. Since containers can be considered self-contained units, each of which fulfills a specific function, they greatly simplify development and operating processes, while enhancing the quality of the service provision. This, in turn, makes faster rollouts and updates possible. Taken together, this results in greater efficiency, which is the primary goal of DevOps in the first place.

What often goes unnoticed, however, is the fact that while containers seem to be an all-purpose tool, they were not primarily developed as a security feature. To ensure containers and container orchestration do not become your own worst enemy when it comes to cyber-attacks, there are a few factors to keep in mind when using Dockers, Kubernetes, etc., including the following:

1. **Containers need to stay "light"**

Security risks can be minimized by not using containers for purposes they were not designed for and by only keeping software that is actually needed. The rule of thumb here: The more software found in a container, the greater the potential field of attack is and the more options an attacker has.

2. **As many rights as necessary – as few rights as possible**

Containers should always be operated with minimal rights. Determining which rights are necessary for each party involved is often time-consuming and is not easy. However, that effort is necessary and definitely worthwhile. Especially since that is the only way to prevent attackers from obtaining every single hidden authorization that has been granted if they do manage to take over a container.

3. **Network segmentation is mandatory for container orchestration too**

A flat, unsegmented network sounds enticing and is easy to put in place as well. However, such networks also make it easier for an attacker to move laterally within the network. Network segmentation, meaning splitting a network into separate, logical areas, makes it more difficult for an

attacker to gain access to other systems. A carefully considered network segmentation is thus not only mandatory in traditional networks, but for container orchestration as well.

Conclusion

Once the decision to use container and orchestration technologies for software development has been made, it is important to take security aspects into consideration before introducing those technologies. A solid plan is essential here. In addition, security must be maintained and constantly upgraded throughout the entire life cycle of the container. To do so, everyone involved must be aware of which requirements need to be met and must also have the know-how necessary to realize those requirements. Since it is not just the applications and the technologies employed that are constantly advancing, but attack techniques as well, it is absolutely essential to constantly adapt security requirements to the latest conditions.

Event announcement regarding it-sa 2019

msg will be represented once again at this year's it-sa – Europe's largest IT security fair – from October 8th to the 10th at the convention center in Nuremberg. Representatives of msg will be available for questions and discussions in **Hall 10.0, Booth 202.** Jan Eltner, Business Consultant at msg will be holding a presentation on container security on October 8th from 3:30 – 3:45 PM in Forum 10.0.

msg

msg is an independent, international group of companies with more than 7,500 employees around the world. The group of companies offers a holistic service spectrum of creative, strategic consulting and intelligent, sustainable and value-added IT solutions for the following industries: automotive, financial services, food, insurance, life science & healthcare, public sector, telecommunications, travel & logistics, as well as utilities, and has acquired an excellent reputation as an industry specialist over the course of almost 40 years in business. Within the group, independent companies cover the wide variety of industry and issue-based competence: msg systems ag forms the core of the company group and works in close cooperation with the subsidiaries, both on a business and organizational level. This allows the competence, experience and know-how of all the members to be bundled into a holistic solution portfolio with measurable added value for its customers.

msg holds sixth place in the ranking of IT consulting and system integration companies in Germany.

For additional information:

msg systems ag
Irina Hofschroeer
Robert-Bürkle-Str. 1
85737 Ismaning/Munich

Tel. +49 89/ 961 01 1650
Fax +49 89/ 961 01 1113
E-mail: irina.hofschroeer@msg.group

Other press-related releases are available at www.msg.group/newsroom.