KubeOps

Security checklist for your Kubernetes infrastructure

The guide for more security & compliance

Security checklist for your Kubernetes infrastructure

Challenges in KRITIS companies

As the person responsible for IT security, especially in critical infrastructures (KRITIS), you are faced with the challenge of managing Kubernetes container systems while maintaining the highest security standards. In view of the current threat situation and the increasing complexity of IT environments, we have developed a special checklist to help you systematically assess and optimise the security of your container infrastructure.

Focus on security standards

Based on the current security standards of the German Federal Office for Information Security (BSI), the NIS Guideline (NIS 1) and the revised NIS 2 Guideline, this checklist guides you through the key security aspects of Kubernetes containers and explains their significance. It helps you to identify security gaps, implement best practices and fulfil legal requirements.

Strategies for the secure operation of Kubernetes containers

Our goal is to support IT managers in reducing the complexity of IT operations, meeting increasing security and compliance requirements and setting up Kubernetes applications in a secure and stable manner. We help software suppliers to focus on the development of their applications without having to invest additional resources in the container infrastructure and to prepare their customers technically so that they can use containerised software or managed services securely.

Basic security check

Do you only use distroless containers?

Use distroless containers to minimise the attack surface. These containers only contain the most necessary runtime environment and fulfil the security requirements of the BSI basic protection.

Are your applications fully statically compiled?

Static compilation avoids problems with dynamic libraries and increases security by reducing dependencies. This is recommended by NIS 1.

Is your image stack fully hardened?

Hardening the image stack protects against known vulnerabilities and unauthorised changes. This is a must according to NIS 2 requirements.

Integrated package management

Do your packages contain all the necessary artefacts without external dependencies?

Independent packages reduce attack vectors through external dependencies and improve the security situation as described in the BSI basic protection.

Are your packages fully configurable, including the use of Helm charts?

Configurable packages allow for flexible customisation and increase security and management efficiency, which is supported by NIS 2.

Is the versioning of your packages clear and traceable?

Unambiguous versioning is crucial for the traceability and management of security updates, in accordance with the requirements of BSI Grundschutz.

Do you use fixed references via SHA keys to ensure consistency?

Fixed references ensure the integrity of the packages and prevent tampering. This corresponds to the best practices of NIS 1.

Baseline level security measures

Are all parameters set to the highest security level?

Set all parameters to the highest security level to minimize the risk of security gaps, as prescribed in the BSI baseline protection.

Have you integrated all necessary operational parameters?

Full integration of operational parameters ensures the operational readiness and security of the infrastructure. This is a requirement of NIS 2.

Is your documentation complete and up-to-date?

Up-to-date documentation is essential for traceability and secure operation, as required by BSI baseline protection.

Security-adapted packages

Have you completely removed unused code and applied secure coding practices?

Remove unused code to reduce the attack surface and improve security. This is required by NIS 1.

Do you use ConfigMaps and Secrets for all credentials and certificates?

Use ConfigMaps and Secrets to protect sensitive data and comply with NIS 2 security requirements.

Have you fully implemented Role-Based Access Control (RBAC)?

RBAC protects against unauthorized access and is a proven security measure according to BSI Grundschutz.

Do you fully apply Ingress Network Policies?

Control network access through Ingress Network Policies to increase security. This is a requirement of NIS 1 and 2.

Supply chain security

Do you only use minimal base images that are not outdated?

- Minimal base images reduce the attack surface and comply with the recommendations of BSI Grundschutz and NIS 2.

Are your container images created entirely from open source software?

- Create your container images from open source software to increase transparency and security. This is required by NIS 1.

Do you fully validate your container images using checksums?

- Checksum validation ensures the integrity of the images and is a fundamental requirement of the BSI basic protection.

Do you perform daily scans and removal of critical vulnerabilities?

- Regular vulnerability scans are crucial for early detection and remediation of vulnerabilities according to NIS 2.

Operational readiness

Are your ingress and proxy servers fully integrated?

- Integrated ingress and proxy servers ensure the secure and efficient management of data traffic, as recommended in BSI basic protection.

Do you make full use of structured labels and comprehensive monitoring?

- Full labeling and monitoring are crucial for the overview and security of the infrastructure, as required by NIS 1.

Have you fully implemented liveness and readiness probes?

- Health checks are essential for operational readiness and availability, as required by BSI Grundschutz and NIS 2.

Are you fully following best practices for scalability and support?

- Best practices ensure a scalable and supported environment. This is recommended by NIS 2.

Minimum requirements for delivery

Is the documentation of the tools and system libraries used complete?

Complete documentation is essential for traceability and maintenance, as stipulated by the BSI basic protection.

Do you carry out a complete vulnerability scan before delivery and log the results?

Pre-delivery vulnerability scans ensure that there are no known vulnerabilities. This is a requirement of NIS 1.

Do you completely eliminate all critical vulnerabilities before delivery?

Complete vulnerability remediation minimizes the risk of security incidents, as required by BSI Grundschutz and NIS 2.

Inspection requirements upon receipt

Do you fully validate the hardening measures using the dual control principle?

Validation by the dual control principle ensures that the security measures have been implemented correctly. This is a best practice according to NIS 1.

Do you complete the validation checklist in full?

Completely working through the checklist ensures that all security requirements are met, as recommended by the BSI basic protection.

Do you fully document all deviations and develop solutions?

Documenting deviations and solutions ensures the continuous improvement of security measures, as required by NIS 2.

Do you fully adapt and re-validate?

Re-validation after adjustments ensures that the security measures are effective. This is recommended by BSI Grundschutz

KubeOps

Summary and recommendations for action

This checklist helps you to systematically assess and continuously improve the security of your KRITIS infrastructure. By implementing the listed security measures, you can effectively protect your container infrastructure against current and future threats. In this way, you can ensure a robust and resilient IT environment that meets the high requirements for critical infrastructures.

Secure KRITIS infrastructure with customized solutions

Let's talk about your current Kubernetes usage and the challenges of managing and securing your container infrastructure during a free consultation. Together, we will determine your technological and operational requirements and show you how our Managed Kubernetes Service (MKS) can help you to ensure a highly secure, stable and efficient IT infrastructure. We will also be happy to answer your specific questions and develop suitable options for your situation. In this way, we support you in achieving your goals and optimally securing your KRITIS infrastructure.