plusserver

NIS2 in a Nutshell

Who is affected? What needs to be done?

What is NIS2?

Network and Information Security Directive 2 (NIS2)

To be transposed into national law by 17.10.2024	Appropriate security measures for organizations in critical sectors	Better cooperation among EU member states to strengthen cybersecurity in Europe	Sanctions and heavy fines for violations

Who is affected by NIS2?

Provision of services in the EU
50 employees or at least €10 million in revenue, or special cases regardless of size

Essential entities	Important entities
Energy	Postal and courier services
Transport	Waste management
Banking, Financial market infrastructures	Manufacture, production and distribution of chemicals
Health	Production, processing and distribution of food
Drinking water	Manufacturing
Waste water	Digital providers
Digital infrastructure	Research
ICT service management (B2B)	
Public administration	
Space	

Sanctions for violations

At least ten million euros or 2 percent of the previous year‘s worldwide revenue	At least seven million euros or 1.4 percent of the previous year‘s worldwide revenue

What needs to be done (in brief)?

Risk assessments	Identify your organization's unique threats and vulnerabilities by conducting regular risk assessments.
Security measures	Implement appropriate state-of-the-art security measures, including access controls, encryption, and monitoring.
Incident management	Create the basis for effective prevention, detection and management of cyber incidents through 24/7 monitoring of the infrastructure.
Incident response plan	Create a well-thought-out incident response plan to ensure you can respond effectively to incidents.
Training and awareness	Train your employees and increase their awareness of security risks. Communicate best practices to minimize human error.
Compliance management	Stay on top of the latest cybersecurity regulations and ensure your organization is always compliant.
Supply chain management	Just as relevant as your own security measures are the measures taken by your suppliers. Pay particular attention to certifications such as ISO 27001 and, in the case of cloud providers a BSI C5 attestation.
Business continuity management	Implement a disaster recovery strategy, e.g. using cloud resources.
External help	You should also contact external consultants and solution providers to ensure that you meet all the requirements of the NIS2 directive.

How can plusserver help?

Security consulting
+ Detailed conception and design of security measures and architectures
+ Pentests and audits

Security solutions
+ SOC as a Service
+ EDR as a Service
+ Vulnerability management
+ Next Gen Firewall
+ DDoS protection
+ Backup/disaster recovery

Certified infrastructure
+ Locations in DE
+ ISO 27001
+ BSI C5 (Type-II)

Contact us for a personal consultation!

› **Get advice now**

plusserver
A sovereign, future-proof and secure cloud.

We offer German companies a sovereign and vendor-independent foundation for their digital business processes. On our secure, scalable cloud platforms, customers can implement future-proof and cost-effective digital applications. We advise our customers on cloud architectures and the integration of existing IT environments. Our approach is fast, dynamic and always personal.

Do you have any questions?
Feel free to contact us.
We are here to help - quickly and easily.

+49 2203 1045 3500
sales@plusserver.com

BSI C5 CLOUD SECURITY · DATENSCHUTZ IDW PH 9.860.1 · ISAE 3402 · gaia-x · Sovereign Cloud Stack · TÜV SÜD ISO 9001 · TÜV SÜD ISO 27001 · more security with JAN-2024 PCI DSS compliant