infinigate
spark your growth

NIS2
Whitepaper

NIS2 is coming
Why you should act now

NIS2 - the Network and Information Security Directive - is a revision of the NIS Directive, which came into force in 2016, with the aim of strengthening cybersecurity resilience across the EU.

The revision tightens reporting requirements and introduces stricter control measures and enforcement provisions. By 17 October 2024, the NIS2 Directive will be a requirement across all EU member states. Despite the urgency – businesses still have many questions.

Distributors like Infinigate are committed to supporting the implementation of NIS2 by offering a broad choice of cybersecurity solutions and services in collaboration with vendors and resellers.

Supporting NIS2 implementation

In Germany, NIS2UmsuCG, the local directive governing the implementation of the EU NIS2 to strengthen cyber security, is already available as a draft and defines EU-wide minimum standards that will be transferred into national regulation.

It is estimated that around 30,000 companies in Germany will have to make changes to comply. However, only a minority has adopted the measures mandated by the new directive so far. Sometimes, symbolic measures are taken with little effect. In view of the complexity of the NIS2 requirements, the short time in which they are to be implemented and the need for holistic and long-term solutions, companies need strong partners who can advise on how to increase their cyber resilience. Often, the challenge is finding IT security experts available to provide support.

As a cybersecurity powerhouse and specialist for IT and Operational Technology (OT), Infinigate offers a large portfolio of cybersecurity solutions that can be deployed to achieve compliance with NIS2 regulations. Additionally, cybersecurity experts are on hand to support channel partners in acquiring the necessary know-how to provide customers with holistic advice - from risk evaluation to mapping of NIS2 requirements and solution implementation. For resellers who lack the necessary resources or prerequisites to offer service packages to their customers, Infinigate provides white-label managed services that can be purchased and customised to suit the local clientele.

A proactive approach

It is recommended that resellers address the topic of NIS2 early on, from the directive to the implementation, to avoid slipping into catch-up mode. Those who are proactive today and have a distributor who can support, can build a strong business model and exploit the growth opportunity and related cross-selling potential. Customers also need to act with urgency – especially in view of the frequency and severity of current cyberattacks, which NIS2 is formulated to counteract.

Who is affected?

The NIS2 directive coming into force in autumn 2024 will apply to organisations across 18 sectors with 50 or more employees and a turnover of €10 million.

Additionally, some entities will be regulated regardless of their size – especially in the areas of 'essential' digital infrastructure and public administration.

The following industry sectors fall under the 'essential' category:

- Energy
- Transport
- Banking and finance
- Education
- Water supply
- Digital infrastructure
- ICT service management
- Public administration
- Space exploration and research
- Postal and courier services
- Waste management
- Chemical manufacturing, production and distribution
- Food production, processing and distribution
- Industry & manufacturing (medical devices and in-vitro, data processing, electronics, optics, electrical equipment, mechanical engineering, motor vehicles and parts, vehicle manufacturing)
- Digital suppliers (marketplaces, search engines, social networks)
- Research institutes

It's worth bearing in mind that NIS2 regulations apply not only to companies, but also their contractors.

Good to know: The "size-cap" rule

The "size-cap" rule is one of the innovations that come with NIS2 and is intended to level out inequalities linked with varying requirements and risk profiles, budgets, resources and expertise. The regulation is intended to enable start-ups and medium-sized companies as well as large corporations to be able to implement the security measures required by NIS2.

You can get NIS2 compliance tips here: nis2-check.com

NIS2 in a nutshell

Companies are required to register with the BSI (Federal Office for Information Security), for their relevant areas. A fundamental rule is that any security incidents must be reported immediately.

The strict security requirements mandated by NIS2 include the following:

✓ Risk Management: identify, assess and remedy

Affected companies are required to take appropriate and proportionate technical, operational and organisational measures. A holistic approach should ensure that risks to the security of network and information systems can be adequately managed.

✓ Security assessment: a self-analysis

Security assessment would answer questions such as: what vulnerabilities are there in the company? What is the state of cyber hygiene? What security practices are already in place today? Are there misconfigured accounts that could be vulnerable to data theft or manipulation?

✓ Access management: protecting privileged accounts

Companies covered by the NIS2 scheme are encouraged to restrict access to administrator-level accounts and change administrative passwords regularly. This will lower the risk of network cybersecurity breaches threatening business continuity.

✓ Closing the entry gates: ransomware and supply chain security

One of the main concerns of the NIS2 directive is proactive protection against ransomware. Endpoint security solutions can help here. Employee training is another necessary step to create risk awareness and help identify and prevent cyber-attacks. The focus here should be on best practices in handling sensitive data and the secure use of IT systems.

Supply chain vulnerability is a major area of concern. Companies need to ensure that the security features and standards of the products and services they purchase meet current security requirements.

✓ Zero tolerance strategy: access control and zero trust

In a world where corporate boundaries are increasingly blurred due to digitalisation, cloud infrastructures and decentralised working models, perimeter-based architectures have had their day. A zero trust concept provides multiple lines of defence, relies on strong authentication methods and threat analysis to validate access attempts.

✓ Business continuity: prepared for emergencies

Business continuity management measures are essential to ensure that critical systems can be maintained in the event of an emergency. These include backup management, disaster recovery, crisis management and emergency plans.

Our vendors

As an EMEA cybersecurity powerhouse, we solve your customers‘ critical security, network and cloud challenges and sustainably to promote their growth.

Vendors in UK

A10
ABSOLUTE
ARISTA
ARMIS
Barracuda
Cambium Networks
CATO NETWORKS
cybereason
ENTRUST
EXAGRID
exinda
Extreme networks
GFI Software
Gigamon
GitHub
HID
iboss
ivanti
JUNIPER NETWORKS
KnowBe4 Human error. Conquered.
NOKIA
nuix
PENTERA
peplink
Progress
riverbed
safend a SuperCom company
SecurEnvoy A Shearwater Group plc Company
SIMSPACE
smartoptics
SONICWALL
Tintri
tripwire
Trustwave
virtana
VECTRA
WatchGuard
WIRE TECHNOLOGIES
yubico

Vendors in Germany

A10
ABSOLUTE
addon
ARMIS
HPE aruba networking
Barracuda

Bitdefender
Cambium Networks
CATO NETWORKS
CHECK POINT YOU DESERVE THE BEST SECURITY
CLOUDFLARE
conpal

corelight
cybereason
CYCOGNITO
CYREBRO
datto A Kaseya COMPANY
DE CIX

deep instinct
DocBee
dogado.partners
ENTRUST
Extreme networks
exterro

Forcepoint
FORTINET
GFI Software
HID
HORNETSECURITY
IACBOX Internet Access Control

illumio
imperva
ITGlue WE ♥ DOCUMENTATION
ivanti
JUNIPER NETWORKS
kaspersky

liongard
lywand software
macmon intelligent einfach
N-ABLE
NETSCOUT
netwrix

NOKIA
OneSpan
Progress
ProLabs
RACKMOUNT
Radiflow

radware
RAPID7
RapidFireTools
riverbed
RUCKUS COMMSCOPE
securonix

SentinelOne
SEPPMAIL
Skyhigh Security
skykick
solarwinds
SONICWALL

sycope
SYSTEMHAUS ERP & CRM für den IT-Channel ONE
Team FON
THALES Building a future we can all trust
Tintri
Trellix

tripwire
tufin
txOne networks
VARONIS
VECTRA
VERSA NETWORKS

WatchGuard
yubico

Infinigate UK Ltd
First Floor, 6 – 8 Bonhill Street
London EC2A 4BX
United Kingdom

T +44 207 593 3290
sales@infinigate.co.uk
www.infinigate.com

infinigate
spark your growth