SSH

Securing Communications for NIS2 Compliance

Practical guide

Index

Introduction 3

What has changed between NIS and NIS2? 4

Why should EU organizations care? 4

Why should non-EU organizations care? 5

How can we at SSH help you comply with NIS2, CER, and other regulations & mandates? 5

Hybrid cloud security (paragraphs 33, 34, and 35) 6

Privileged access, credential, and admin-level access management & path to passwordless (paragraphs 44 and 49) 7

Sharing confidential, classified, restricted and secret information securely (paragraphs 45, 96, and 118) 7

Protecting utilities and other critical infrastructure (paragraph 53) 8

Proactive and defensive cybersecurity (paragraphs 57, 98, and 105) . . . 9

Protect your data in transit, in use, and at rest (paragraph 78) 10

Mitigate the risk of the supply chain, outsourced service providers nd third parties (paragraphs 83, 84, 85, 86, and 88) 10

Strong identity combined with Zero Trust authentication principles (paragraph 89) 11

Incidence response, reporting, and auditing (paragraph 101, 102, and 103) 11

Conclusion 12

Switch on secure communications between people, clouds, data centers, systems, networks, and applications 12

Introduction

The Network and Information Security (NIS) Directive, created in 2016, was the first set of cybersecurity obligations that covered the entire European Union. Its goal was to build a systematic set of rules, guidelines and laws for a consistent approach to network and information system security within the EU.

Since then, there's been more activity. The NIS2 Directive repeals the current NIS Directive and creates a more extensive and harmonized set of rules on cybersecurity for organizations carrying out their activities within the European Union. The CER Directive repeals the European Critical Infrastructure Directive and brings with it new, stronger rules for the cyber and physical resilience of critical entities and networks. The main goal of CER is the help critical infrastructure to run without disruptions and protect the physical networks from digital threats.

NIS2 also puts a lot of emphasis on cooperation and information sharing within the EU. For this purpose, the EU has established the European Network of Cyber Crisis Liaison Organizations (EUCyCLONe) to boost coordinated management of large-scale cybersecurity incidents at the EU level.

What has changed between NIS and NIS2?

For a more comprehensive look at the changes, check out our Guide to NIS2 Directive. However, some of the most important points include:

- NIS2 applies to a wider range of industry sectors, including:
  - public organizations both at government and local level
  - energy
  - transportation
  - water facilities
  - ICT service management
  - waste management
  - manufacturing facilities
  - postal services
  - and more
- Several new requirements for active security controls and preventive measures
- More obligations for incident response and crisis management reporting
- Enhanced emphasis on the subcontractors, third-party, service provider, and supply chain security
- Focus on the hybrid cloud security
- Requirement to protect sensitive information when it is shared
- Best practices, recommendations, and a call-to-action for cybersecurity training within organizations

Why should EU organizations care?

It's a law, not a recommendation

It is important to understand that NIS2 is not a recommendation or a regulation, it's a law that is enforced throughout the Union with administrative sanctions and fines for failures to comply.

Failure to comply costs organizations

Penalties are up to €10,000,000 or 2% of the annual global revenue of the business or organization. Furthermore, any organizations found infringing the Directive are subject to rigorous audits for years to come to demonstrate compliance.

NIS2 is already in force, no time to delay

Yes, the law is already in force. EU member states need to tie NIS2 into their national legislation by October 17, 2024, after which it will also be overseen and sanctioned at member state level. The time to act is now.

Leaders have personal liability

What's more, there's the liability of natural persons holding representation or senior management positions, including the Board of Directors, the company leadership team, and the Chief Executive Officer.

Leaders have personal liability

What's more, there's the liability of natural persons holding representation or senior management positions, including the Board of Directors, the company leadership team, and the Chief Executive Officer.

There's a burden of proof

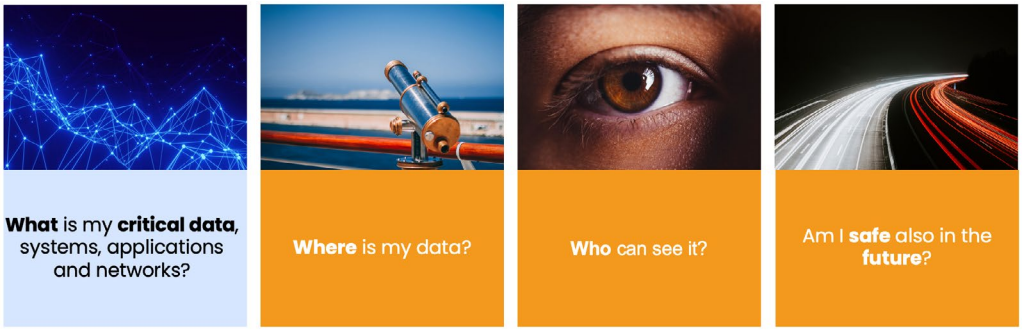
Security audits will require a demonstration of compliance with NIS2. Organizations need to show how they have set up their environment so that it adheres to NIS which in turn requires a good understanding of the organization's security posture.

Why should non-EU organizations care?

The answer is simple. If your company or organization has any kind of business within the EU and it falls under the NIS2 scope, all the consequences of non-compliance apply to your organization and its leadership team.

How can we at SSH help you comply with NIS2, CER, and other regulations & mandates?

We at SSH believe that there are four fundamental questions all businesses and organizations should be able to answer to be secure and compliant with NIS2. They are illustrated in the following picture



With this guide, we will show you what are the key NIS2 paragraphs for your organization to consider and how we at SSH can help you to comply and address the following topics:

1. Hybrid cloud security
2. Privileged access, credential, and admin-level access management & path to passwordless
3. Sharing confidential, classified, restricted and secret information securely
4. Protecting utilities and other critical infrastructure
5. Proactive and defensive cybersecurity
6. Protect your data in transit, in use, and at rest
7. Mitigate the risk of the supply chain, outsourced service providers and third parties
8. Strong identity combined with Zero Trust authentication principles
9. Incidence response, reporting, and auditing

1 Hybrid cloud security (paragraphs 33, 34, and 35)

Summary

These paragraphs focus on defining the different types of cloud (Amazon AWS, Microsoft Azure, and Google Cloud) and on-premise services that need to be protected, including the various ways and endpoints used to access these services.

- On-premises data centers
- Virtual servers
- Distributed cloud
- New innovative technology, like edge computing

How can SSH help?

Our Zero Trust Suite is a comprehensive set of solutions for building secure communication channels and access gateways in multi-cloud, hybrid cloud, or on-premise environments – or any combination of them. As pioneers in secure communications, we have the solutions to secure both the customers' installed base (often mostly on-premises) while helping them on their journey to modern, cloud-based technologies (including distributed cloud, containers, or Kubernetes).

Examples include:

- **Auto-discovery of cloud and on-premises assets:** Get a global view on your asset inventory automatically for easy access management.

- **Centralized access management to the hybrid cloud:** Use the same, consistent and coherent logic to access any target in the hybrid cloud, regardless of the vendor.
- **Application security:** When you are hosting privileged applications (like GitHub repositories) or business applications (like your CRM), we can secure access to all of them.

2 Privileged access, credential, and admin-level access management & path to passwordless (paragraphs 44 and 49)

Summary

These two paragraphs refer to the importance of "privileged management interface" and related credential and admin-level access management. Every organization has administrative users with access to privileged accounts that grant elevated, often broad and risky access to a large segment of the network.

How can SSH help?

SSH's Zero Trust Suite includes enhanced Privileged Access Management features, such as:

- Disarming privileged accounts while they are inactive to protect them from misuse
- Logging, monitoring, recording and auditing sessions for forensics and compliance
- Restricting access to the minimum needed to get the job done to limit the impact radius of admin accounts
- Path to passwordless: Mitigate the risk of shared credentials, such as passwords and authentication keys, by managing them or going for just-in-time access without passwords and keys

3 Sharing confidential, classified, restricted and secret information securely (paragraphs 45, 96, and 118)

Summary

This paragraph refers to the importance of sharing incident-related and other critical information between relevant stakeholders and authorities while respecting data protection and privacy laws. Secret, confidential and restricted level information can only be shared using authorized solutions.

How can SSH help?

SSH's Zero Trust Suite contains secure business communication solutions that allow organizations to build authorized and compliant channels for sharing sensitive information:

- Verify sender/recipient and all collaborators when sending emails, using workspaces, signing documents, or collecting information using forms.
- Complement your existing email services with government-grade security and full encryption from sender to recipient.
- Build communication channels allow you to be in complete control of your data without using any outsourced services or servers, like emails services.
- Grant read-only, notification-only, edit, and full-access rights to sensitive information as needed.
- Ensure that instant messages containing secrets are shared with officially approved solutions with robust security features.

4 Protecting utilities and other critical infrastructure (paragraph 53)

Summary

This paragraph highlights the importance of protecting utilities and other critical infrastructure providers from cyberattacks. Businesses in operational technology (OT) tend to have low cyber-awareness, lack remote IT security, and experience an increased level of threats, such as ransomware. This is because these companies are taking the first steps in digitalizing their services and networks.

How can SSH help?

SSH's Zero Trust Suite includes full-scale secure remote access management tools purpose-built for OT:

- Support for IT protocols like SSH, RDP, HTTPS, and VNC for access. Remote access using any TCP/IP protocol prevalent in OT by granting access on a network level. Support for protocols or targets using OT proprietary technology, such as:
  - » Ethernet IP
  - » Profinet
  - » Modbus TCP
  - » MTTQ
  - » OPC-UA
- Built-in workflows and out-of-the-box integration for ticketing system for approving jobs on-site and off-site

- Logging, monitoring, recording and auditing sessions for forensics and compliance with not only NIS2 but ISA/IEC 62443, ISO 27001, and NIST
- No IT expertise required: in-house and outsourced maintenance engineers log into an easy-to-use interface that grants access only to their available targets every time

5 Proactive and defensive cybersecurity
(paragraphs 57, 98, and 105)

Summary
These paragraphs are an important reminder that cybersecurity is more than responding in a time and correct fashion after a breach has happened but building a defensive strategy and a mindset that fosters the culture of preventing breaches from taking place. It is even more important to prevent and defend than it is to respond and report.

How can SSH help?
We at SSH have been promoting the idea of defensive cybersecurity for a while already. Some key highlights from our portfolio that can help you on your journey toward this goal include:

- Risk assessment services to gain a good understanding of your current security posture
- Encrypting all communications, whether they are:
  - Human-to-human (H2H)
  - Application-to-application (A2A)
  - System-to-system (S2S)
  - Server-to-server
  - Data center-to-data center
  - Cloud-to-cloud
  - Any combination of the above
  - Human to application, system, server or database
- Ensuring critical credentials that include passwords and keys are managed
- Implementing methods where permanent authorizations, like passwords and keys, are no longer necessary, but access is granted just-in-time for the session without permanent credentials that can be shared, lost, stolen or misused
- Easy-to-use solutions that automate linking the identity with the right level of access to the right target
- Applying multi-factor authentication, biometric authentication, and single sign-on methods for security
- User and entity behavior analytics (UEBA) to automatically stop anomalous activity, for example, based on location, time, or target

6 Protect your data in transit, in use, and at rest (paragraph 78)

Summary

This paragraph is a reminder that data has different lifecycles, basically when it is in transit, in use, or at rest. Regardless of the intended use, it should be protected.

How can SSH help?

Our solution portfolio offers a comprehensive solution for all the stages of the data lifecycle:

- Secure remote access management when servers, databases, network devices or other targets are being configured, upgraded, maintained
- Building encrypted communication pipelines when data is being transferred between servers, applications, data centers or using other automated automated/batch file transfers
- Establishing authorized communication channels for sharing sensitive data with external stakeholders
- Protecting sensitive information with strong encryption when it is stored
- Building quantum-safe tunnels for your most critical connections, for example between OT sites

7 Mitigate the risk of the supply chain, outsourced service providers and third parties (paragraphs 83, 84, 85, 86, and 88)

Summary

These paragraphs refer to different types of supplies, service providers, subcontractors and third parties who all have access to your network and critical data.

How can SSH help?

We at SSH have long-standing expertise in secure communications and secure remote access management, including:

- Tailor-made access management solution for Managed Service Providers (MSP) and Managed Security Service Providers (MSSP) who all maintain a critical part of the customer network and data
- Tailor-made solution for on-site and off-site maintenance engineers in OT for remote and local access
- Easy to use toolset for instant onboarding of subcontractors who need access to critical system

- Automatic offboarding of third parties when they leave a project
- Full audit trail of activities with the possibility to record sessions, monitor them live and instantly terminate them if needed
- Hiding the secrets needed to access a target from the third party and ensuring that they don't even need to handle any permanent credentials that could be shared

8 Strong identity combined with Zero Trust authentication principles (paragraph 89)

Summary

This paragraph highlights the importance of preventing access without identity and applying Zero Trust principles when building security controls. The Zero Trust principle states "Don't trust, verify".

How can SSH help?

As the name implies, our Zero Trust Suite has been designed around the idea of not giving any ID a permanent authorization to a target:

- All access is temporary by default and is verified each time a new session is established.
- Grant access and authorization only just at the time when it is needed.
- Always assign strong identity to every session, whether the user is a human or machine.
- When possible, use just-in-time access together with passwordless and keyless authentication to remove the risk of permanent credentials.
- When passwords and authentication keys are needed (often the case in traditional environments), vault and rotate the credentials.
- Assume that the internet, intranet, and extranet are all equally unsafe and encrypt all sessions.
- Apply biometric and multi-factor authentication methods to particularly sensitive or critical sessions and monitor them for four-eyes inspection.

9 Incidence response, reporting, and auditing (paragraph 101, 102, and 103)

Summary

These paragraphs emphasize the importance of swift reporting of cybersecurity incidents without delay to mitigate their impact radius. In addition, proper audit trail will help understand why a breach took place to stop such incidents from happening in the future.

How can SSH help?

Zero Trust Suite has extensive reporting and dashboard features, along with integrations with other security systems for further analysis:

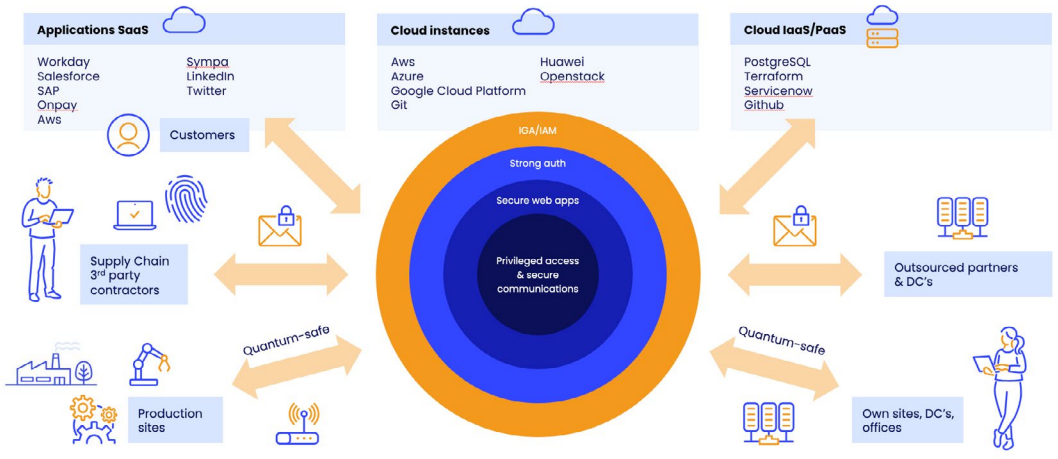
- A solid audit trail of activities for all sessions and connections, whether machine or human initiated.
- Dashboards to view audit those events
- Session recording and monitoring available when necessary
- Dashboards to demonstrate the use of authentication keys that grant access to your critical targets.
- Up-to-date view to your global on-premises and cloud estates.
- Integration with Security Information and Event Management (SIEM), Security orchestration, automation and response (SOAR) and Security Operations Center (SOC) to send our data for further analysis

Conclusion

Switch on secure communications between people, clouds, data centers, systems, networks, and applications

Secure communications have transcended artificial borders. Traditional enterprise network security solutions, like firewalls, demilitarized zones (DMZ), or VPNs grant too broad access or are hard to configure to be flexible and granular.

Your applications, servers, cloud, data centers, networks, network devices, and industrial targets are dispersed in an extended ecosystem. There are no safe zones that exist conveniently behind a wall: the intranet, extranet, and internet are by default equally unsecure.

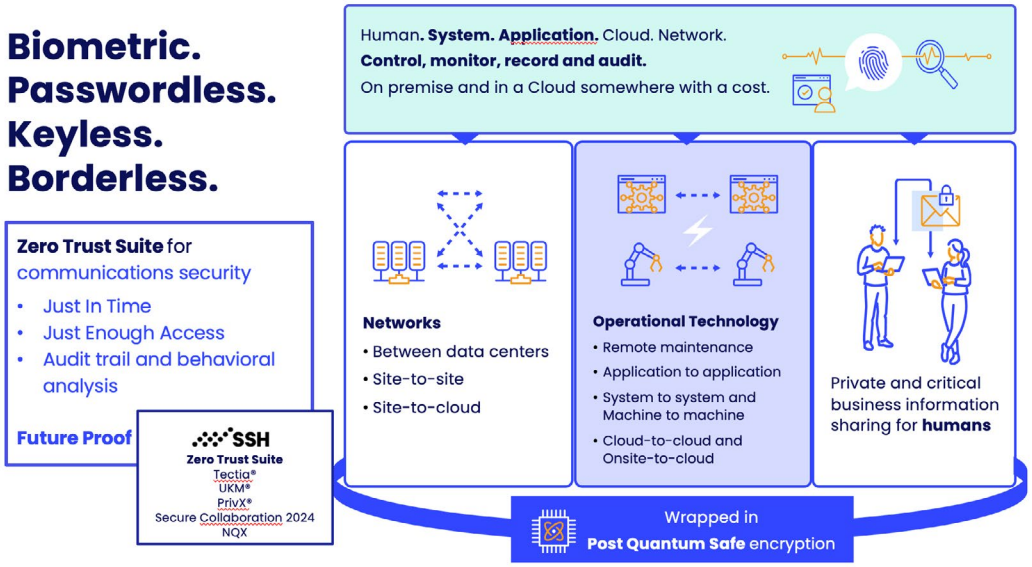


We at SSH secure communications between people, clouds, data centers, systems, networks, and applications. We help you identify every access, secure your credentials, and audit every session for forensics and compliance.

Our Zero Trust Suite is a modular set of software solutions that can help you navigate through the key requirements defined in the NIS2 Directive and other regulations.

We are called SSH Communications Security for a reason: we laid the foundation for secure communications with the invention of the Secure Shell protocol, the defacto method for securing application-to-application and human-to-application communications. Ever since, we expanded our portfolio and expertise to meet the cybersecurity needs of some of the most demanding customers in the world, including a host of Fortune 500 luminaries.

[Learn more about our Zero Trust Suite >>>]



Don’t hesitate to contact us to book a meeting.

We are happy to help you on your journey towards NIS2 compliance.

BOOK A MEETING

We'd love to hear from you!

Get in touch with our experts around the world.

GLOBAL HEADQUARTERS

Helsinki

SSH COMMUNICATIONS
SECURITY CORPORATION
Karvaamokuja 2b, Suite 600
FI-00380 Helsinki
Finland
+358 20 500 7000
info.fi@ssh.com

US HEADQUARTERS

New York City

SSH COMMUNICATIONS
SECURITY, INC.
434 W 33rd Street, Suite 842
New York, NY, 10001
USA
Tel: +1 212 319 3191
info.us@ssh.com

APAC HEADQUARTERS

Hong Kong

SSH COMMUNICATIONS
SECURITY LTD.
35/F Central Plaza
18 Harbour Road
Wan Chai
Hong Kong
+852 2593 1182
info.hk@ssh.com

SSH