Getting started with NIS2 – The Checklist

All EU member states are expected to comply with NIS2 by 2024. This means following specific cybersecurity strategies, establishing competent authorities, and implementing incident reporting mechanisms. NIS2 requires EU member states to cooperate in the sharing of information to safeguard vital assets from cyberattacks.

NIS2 builds on the requirements of the original directive; It aims to protect critical infrastructure and organizations within the EU from cyber threats and achieve a high level of common security across the EU.

To achieve this goal, NIS2 requires member states to take a number of additional measures, including:

- Establishing an incident response plan that coordinates with other member state plans
- Establishing a national Computer Emergency Response Team
- Strengthening cooperation between public and private sector entities
- Improving information sharing between member states

With that in mind, here is a quick checklist to ensure you have everything in place to comply with the NIS2 directive. Simply work your way through and check off the prompts or tasks.

First off - Does NIS2 apply to you? Well, probably, yes!

Are you in one of these industries?

- ☐ Energy
- ☐ Government
- ☐ Other Public Admin
- ☐ Transport
- ☐ Education
- ☐ Police
- ☐ Banking
- ☐ Finance
- ☐ Manufacturing
- ☐ Healthcare
- ☐ Water (Waste/Drinking)
- ☐ Digital Infrastructures
- ☐ Space
- ☐ Postal/Courier
- ☐ General Waste Management
- ☐ Chemicals (Disposal/Production)
- ☐ Science
- ☐ Food Industry

Compliance with NIS2 is not an option. For that you need to meet a set of requirements, however all compliance starts from the ground up before you even get to security solutions and platforms. You have to ensure that your colleagues across the company or organization are aware of what is required of them. This helps to mitigate risk right from the start.

Important to note: Risk management and assessments are an ongoing process. They require a constant. Once one risk assessment is carried out, it is important to schedule regular updates to ensure all steps are maintained.

Consider these as steps. 1. Awareness 2. HR security. 3. Control of assets - Where are they, how many do you have, are they updated? 4. Incident management in a standardised and consistent way. 5. Vulnerability management are your systems updated? 6. Assessment of risk in supply chains. 7. Network security. 8. Security in development processes - Do you know who writes your code, are you sure nobody else wrote some backdoors? 8. Access control, both physical and virtual. 9. Application of encryption where relevant. 10. Contingency planning - What do you do if somebody compromizes your network or steals your data or you get ransomware?

Now for the deep dive

For you:

- ☐ Have you read up on the requirements of NIS2?
- ☐ Do you have a full understanding of key difference between NIS and NIS2?
- ☐ Do you know who is responsible for compliance and who is held liable if you do not comply?
  - ☐ Importantly! Do they know they are responsible?
- ☐ Does your infrastructure have incident response and crisis management capabilities?
- ☐ Now assess how you will handle vulnerabilities and disclosure?
  - ☐ Have you performed an assessment of the risks involved in this?
- ☐ Assess your supply chain is it secure?
  - ☐ Have you assessed the potential risks to your supply chain?
  - ☐ Have you assessed the risks associated to your customers?

For you to help your colleagues:

- ☐ Do you have policies and procedures in place for the assessment of your cybersecurity?
- ☐ Have you carried out cybersecurity training?
- ☐ Have you educated your colleagues on the importance of data handling and compliance?
- ☐ Have you performed a maturity assessment?
- ☐ Do you have a plan moving forward to strategize

Computer Hygiene

Informing the people in your organization of the need to comply with the likes of GDPR and NIS2 is vital. How they handle data at the ground level can have a huge impact on data and compliance. If they do not know how they should handle data and information, or they think they are carrying it out correctly, but they are not. Well, that is an issue.

- ☐ Have you assessed your basic computer hygiene practices?
  - ☐ Are they sufficient in complying with NIS2?
- ☐ Do you have a cybersecurity hygiene policy?
  - ☐ If not have you created a cybersecurity hygiene policy?
  - ☐ Have you distributed it through the company and even at C-Level?
- ☐ Do you have a central security platform?
  - ☐ Can you automate regular tasks?
- ☐ Do you have strict password policies in place for all personnel?
- ☐ Have you ensured you have sufficient multifactor authentication in place?
- ☐ Do you have endpoint protection in place?
- ☐ Have you applied relevant frameworks?
  - ☐ NIST
  - ☐ ISO
  - ☐ CIS
  - ☐ Mitre Att&ck

Cryptography

- [ ] Do you have the collaterals to explain cryptography to those that need it?
- [ ] Have you applied cryptography effectively?

Other

- [ ] Do you have compliant HR practices for cybersecurity?
- [ ] Do you have HR security access and control policies in place?
- [ ] Have you risk assessed your HR security access and control policies?

Failure to comply

- [ ] Are you aware of the consequences of non-compliance?

What the right cybersecurity platform can do to help ensure you meet compliance

- [ ] Do you have sufficient cybersecurity measures in place?
  - [ ] SIEM
  - [ ] SOAR
  - [ ] UEBA
  - [ ] SAP System and Application Security
  - [ ] Endpoint security
  - [ ] Is it a SaaS solution?
    - [ ] Is it a SaaS solution with data residency in the EU?

Reporting

Reports are a requirement of NIS2:

24 hours: Early warning that includes if the incident is caused by unlawful or malicious acts or could have cross-border impact.

72 hours: Notification that includes initial assessment with severity and impact and IOCs. Immediate reports on status updates as requested by authority.

Plus: A final report no later than one month after first notification that includes detailed incident descriptions, types of threat, mitigation measures, and cross-border impact of incidents.

- [ ] Does your security platform provide you with playbooks that automatically gather, convert, and disseminates the information for compliance with reporting requirements?

Incident handling

NIS2 defines incident handling as: any actions and procedures aiming to prevent, detect, analyze, and contain or to respond to and recover from an incident.

- ☐ Do you have one consolidated solution that facilitates incident handling?
- ☐ Do you have sap security in place/ability to report on SAP issues/visibility into SAP systems for monitoring and incident handling?

Further certification and compliance

- ☐ Does your security have Common Criteria EAL3+ certification?
  - ☐ More info go here.
- ☐ Does it adhere to ISO 15408?
  - ☐ More info go here.
- ☐ Does your cybersecurity comply with:
  - ☐ GDPR
  - ☐ Schrems II
  - ☐ CCPA

For more info on NIS2 and how Logpoint can facilitate you in your compliance needs head here.

Download the NIS2 brochure