WP-031-2020

ENCS reply to the consultation on the revision of the NIS Directive

Version 1.0

16 October 2020

This document is shared under the Traffic Light Protocol classification:

TLP WHITE - public

The European Network for Cyber Security (ENCS) is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component, and end-to-end testing, as well as education & training.

ENCS

Introduction

In October 2020, ENCS provided input to the European Commission's NIS Directive Consultation. This paper provides a summary of the ENCS responses.

Since the entry into force of the NIS Directive in 2016, the cyber threat level has increased significantly. Yet, much remains to be done for companies in the EU to counter this development. ENCS emphasizes that it is vital to promote a culture of security across all sectors critical for our economy and society. As risks transcend national borders, cybersecurity measures need to be aligned at the Union level. To achieve this, both the capabilities of Member States and the level of cooperation among them needs to be improved.

On whom should be included

In today's smart grid, everything is connected, meaning that an attacker only needs to look for the weakest link in the chain to cause significant damage. Multiple infrastructures are connected to or integrated in the grid and can cause serious damage to the grid when malicious actors take control. ENCS is strongly supportive of considering all parties critical to the security of electricity supply as Operators of Essential Services (OES), so that they fall under the NIS directive. To date, different approaches to identifying OES are followed in different countries. This leads to a dangerous variety in OES designations and a lack of European harmonization which prohibits a level playing field for security. As cross border dependencies are highly relevant for the energy sector, this can have serious consequences.

ENCS strongly recommends including sub-sectors and cross-dependent parties that can have a significant impact on the security of critical infrastructures in the scope of the NIS Directive. ENCS recommends considering the following parties in particular:

- Distributed Energy Resource operators
- Electric Vehicle Charging operators
- Public telecom networks

To be effective, the NIS Directive's scope does not only have to be complete but also future proof. Given the growing dependence on ICT systems and the internet, the current definitions in Annex II are too restrictive for the energy sector in the future. New stakeholders are emerging due to the introduction of renewables and electric vehicles. These stakeholders may quickly become critical infrastructure, but do not fit in the definitions of Annex II. A more flexible definition focusing on critical business processes is recommended.

On what should be included

Overall, we think the NIS directive has been successful. We see that OES are paying more attention to security, so thatthat in the next few years a reduction of their risk can be expected. As the potential impact of incidents in the energy sector is high, even a small reduction in the likelihood of events gives big societal benefits. Costs might have been lower if the required measures and reporting thresholds would have been clear from the start. Uncertainty about what the directive will require leads to more costs at OES trying to anticipate the requirements.

To further improve security, more harmonization is needed on what measures are implemented under the NIS directive. There is a big variety in scope and maturity of the measures that already exist. Many member states are still elaborating on their precise requirements. However, they need time to build sector-specific security knowledge. Uncertainty over the requirements makes it more difficult for OES to set up an effective program to meet them.

ENCS' advises the Commission to pay special attention to security risk management, vulnerability disclosure and sharing incident information when selecting measures.

Security risk management

To consider technological advances and trends, the EU cybersecurity policy should promote the deployment of security risk management through an Information Security Management Systems (ISMS). This would ensure frequent and adequate evaluation of new threats and risks. For the procurement of energy grid systems, mature security requirements considering the needs and constraints of both grid operators and manufacturers are needed. This should be enforced, and the correct implementation verified through standardized functional and penetration testing.

Requirements on risk management would be preferred over prescriptive requirements on what controls to implement. They offer more flexibility for OES to choose efficient solutions in their specific situation and to react to new developments. But a risk-based approach is hampered by the difficulties of objectively measuring high-impact low-frequency risks. So, some prescriptive requirements could be justified especially for smaller parties. Certification can help, but will only be effective if:

- high-quality requirements are in place on risk management,
- a good certification scheme is in place, matching the needs and constraints of the domain.

Vulnerability disclosure

Based on ENCS' experience in the OT domain, the industry is quite immature when it comes to vulnerability disclosure. Security testing is not common, if it is done, then predominantly by grid operators. The classification of findings is not harmonized and the potential impact on the grid and society is not well addressed. Testing often only happens under strict NDAs prohibiting the sharing and reporting of findings. Contractual frameworks to enforce resolution of the findings are mostly lacking.

To resolve this, ENCS proposes a standard defining security requirements. Additionally, standardized and reproducible testing methods are needed. When tests conducted for manufacturers, rather than grid operators, prove that requirements are met, the test results should be published. For vulnerabilities found by the standardized testing approach, incentives like fines or trade constraints could be considered, if not resolved within fixed timescales.

Sharing incident information

The NIS directive requires that information about security incidents is shared through national CSIRTs. But this has not yet lead to more information about incidents becoming available to OES. Often there is still uncertainty about which incidents need to be reported in the energy sector. The need to report a hack causing a major blackout is clear. However, it is not clear if an incident that could have caused disruption but, in the end, did not, needs to be reported. Similar confusion occurs when incidents are caused by user errors or technical problems. This problem can be traced back to OES' reluctance towards sharing information unless the threshold is clearly passed. They are concerned that information about incidents is used by the competent authority to question whether appropriate measures have been taken. However, this reluctance hampers effective information sharing.

The key to sharing sensitive information is to rely on trust, rather than on a mandate. A trust-based model builds on voluntary sharing, which is consistent with the GDPR concept. Organizations can be incentivized to share more information with cybersecurity authorities voluntarily if win-win situations are created. Authorities must be specific about what organizations get in return for providing information. For example, if intelligence services share new threats and analysis with organizations, what information could organizations provide to intelligence services to support and improve their threat analysis? Can authorities provide support to resolve vulnerabilities when organizations report vulnerabilities?

Regarding the information to be shared, the discussion should go beyond the scope of information authorities require, as the resolution of major incidents cannot be done by authorities alone but require the cooperation of OES. Therefore, the information sharing need amongst OES seems at least equally relevant and is perhaps less complicated due

to national interests/obligations for authorities. The OES in the energy sector would benefit from information on the likelihood of targeted attacks on the energy supply. Individual OES cannot collect enough data on likelihoods to perform quantitative risk assessments and they rarely detect targeted attacks. Aggregated and anonymized data at the EU level could help them make better risk assessments.

The level of information exchange between energy sector companies could be improved as well by supporting a similar trust-based model. Constraints prohibiting the flow of information due to national and/or commercial interests should be removed. Mandated compositions of ISACs and CSIRTs constrain the exchange of sensitive information. Complementary approaches will be required to:

- enable sharing of information critical to incident detection and response,
- share and resolve vulnerabilities.