European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

PREPARING FOR CYBER ATTACKS IN THE ENERGY SECTOR

This is a short ENISA paper for senior management in the EU's energy sector, to support them with raising the level of preparedness and overall resilience in the face of potential cyberattacks.

1. SITUATIONAL PICTURE

The key cybersecurity threats for the energy sector are:

1. **Ransomware continues to be a major threat for all organizations in the energy sector[1] [2]. In the same category are wipers, like NotPetya[3], which scramble or delete data, without a way to recover data.** To mitigate ransomware it is important to have good backup procedures[4], in case data does get encrypted or wiped, and to try to prevent ransomware by hardening the endpoints, hardening web-facing systems, and segmenting the company's network, applying zero-trust principles.

2. **Phishing is still one of the main vectors for all sorts of cyber-attacks, including cyber espionage[5] and ransomware. It is easy for an attacker to craft a good-looking (spear-phishing) email with a malicious link or malware attached.** To prevent phishing, a combination of technical and organizational measures are needed. Technical measures include email filters that scan attachments and rewrite links, email verification (DMARC), marking incoming emails as untrusted, and hardening the endpoints where emails are opened. Organizational measures include educating your employees about social engineering tactics. Awareness is important to create a "human firewall".

3. **Supply chain attacks, like the SolarWinds incident[6], are an increasing threat for organizations in all sectors but particularly operators of critical infrastructure are attractive targets. If suppliers have a low level of cybersecurity protection, they become be an easy entry point into your organization.** Eliminating supply chain attacks is not easy, but companies can reduce their exposure by uninstalling software, disabling unnecessary functions, and including cybersecurity requirements in contracts with suppliers and service providers in their supply chain. ENISA published a comprehensive overview of different supply chain attacks last year[7].

2. CRISIS MANAGEMENT

In case you become aware of cyberattacks targeting your organisation or if you detected a cybersecurity incident, please reach out quickly to your national CSIRT or, depending on the national setup, the dedicated CSIRT for the energy sector. Contact details of CSIRTs across the EU can be found at https://csirtsnetwork.eu/. Make sure you have these communication channels up and running.

[1] https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/
[2] https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html
[3] https://www.cnet.com/tech/services-and-software/uk-said-russia-is-behind-destructive-2017-cyberattack-in-ukraine/
[4] For instance, following the 3-2-1 principle: At least 3 copies, in 2 places, 1 off-site – see; Secure Backups — ENISA (europa.eu)
[5] https://www.bleepingcomputer.com/news/security/cyber-espionage-campaign-targets-renewable-energy-companies/
[6] https://abcnews.go.com/Politics/russian-nation-state-actor-solarwinds-cyberattack-microsoft/story?id=80771329
[7] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

Note that your national CSIRT has access to cross-border cross-EU platforms for operational and technical collaboration and information exchange[8].

Please consult your national legislation and national guidance from authorities on risk management measures, and incident reporting to national authorities and agencies, such as national cybersecurity agencies, sectorial authorities, data protection authorities and law enforcement.

3. PREPAREDNESS QUESTIONS

We shortlist some key questions senior management should ask the relevant information security and risk management functions in their organisation, to understand the overall level of preparedness.

Governance and ecosystem

1. Is there an up to date list of the most critical IT systems and OT systems, and what are the relevant cyber threats that could affect them?
2. Do we have an overall cyber-risk management program (also known as information security management system), and does it cover both IT and OT systems?
3. Do we have a good understanding of our overall ecosystem, our dependencies on other organisations in and outside the sector, our suppliers and vendors?

Protection

4. Do we have a vulnerability management program in place that ensures that all IT and OT systems are timely patched and updated? How does this program cover our legacy systems?
5. Do we have protection in place for remote access of IT and OT systems, such as two-factor authentication, particularly for privileged (administrator) accounts?
6. Do we have segmentation in the organisation's network, and do we implement zero-trust network architecture principles.
7. Is our staff aware of phishing threats and other forms of cyber-attacks? Is there a staff program for training and awareness raising on cyber security?

Defence

8. Do we have clear roles and contact points for incident response, both for IT and OT incidents?
9. Do we have up-to-date incident response plans and procedures? Did we test them recently?

Resilience

10. Do we have appropriate backup and recovery procedures in place?
11. Do we have up-to-date business continuity and contingency plans? Did we test them recently?
12. Do we have crisis management procedures in place, do we know who to contact in case there are attacks or incidents?

For a complete overview of relevant cybersecurity measures, targeted specifically at the energy sector, please consult the NIS Cooperation group technical guideline on the Sectorial implementation of the NIS Directive in the Energy sector which covers the above 4 areas, but in more technical detail and with references to technical standards and industry good practices.

[8] All national CSIRTs in the EU are member of the EU's CSIRTs network, which is a network for cross-border information exchange and collaboration at the technical level. Cyclone is the EU-level crisis management structure for operational collaboration between EU Member States in case of large-scale cybersecurity incidents.