Smart Grid Cyber Security

A EURELECTRIC report

December 2016

EURELECTRIC is the voice of the electricity industry in Europe.

We speak for more than 3,500 companies in power generation, distribution, and supply.

We Stand For:

***Carbon-neutral electricity** by 2050*

We have committed to making Europe's electricity cleaner. To deliver, we need to make use of **all low-carbon technologies**: more renewables, but also clean coal and gas, and nuclear. Efficient electric technologies in **transport and buildings**, combined with the development of smart grids and a major push in **energy efficiency** play a key role in reducing fossil fuel consumption and making our electricity more sustainable.

***Competitive** electricity for our customers*

We support well-functioning, distortion-free **energy and carbon markets as** the best way to produce electricity and reduce emissions cost-efficiently. Integrated EU-wide electricity and gas markets are also crucial to offer our customers the **full benefits of liberalisation**: they ensure the best use of generation resources, improve **security of supply**, allow full EU-wide competition, and increase **customer choice**.

***Continent-wide** electricity through a coherent European approach*

Europe's energy and climate challenges can only be solved by **European – or even global – policies,** not incoherent national measures. Such policies should complement, not contradict each other: coherent and integrated approaches reduce costs. This will encourage **effective investment to** ensure a sustainable and reliable electricity supply for Europe's businesses and consumers.

EURELECTRIC. Electricity for Europe.

Dépôt légal: D/2016/12.105/64

Smart Grid Cyber Security

A EURELECTRIC report *December 2016*

KEY MESSAGES

- The Society is highly dependent on the electrical grid, which has been going through a profound and much necessary digital transformation over the past few years, to be able to address the sector challenges. However, this digitalization process highly increases the exposure of network operators to cyber threats, presenting high risks for both business and society that were not present before. Customers will be the victims of cyberattacks on electric grids with data loss, blackouts and/or invasion of privacy

- Data shows that cyber threats and their impact are rapidly increasing across Europe.1. To achieve cyber security across the electrical grid at European level, network operators should have a well-structured cyber security strategy, based on risk assessment schemes. They should also develop a breach detection and response capability to minimise the damage that a cyber attack might cause. Companies/organisations compliant with these recommendations should be able to raise awareness, in particular within the company's middle and top management.

- As regulated entities that deal with critical infrastructures, DSOs need to develop competencies connected with cyber security in their core business and adopt advanced technologies and mature procedures in order to give a suitable response to any incoming threat. Moreover, European and National legislation could work as an enabler if the Regulator recognises the importance of providing the necessary expenditure for the potentially costly cyber security investments and organisational transformation

- The need to be compliant with the latest cyber security directives2 and guidelines will put pressure on hardware suppliers to take cyber security issues seriously and therefore, sell more secure products, which will benefit the whole market. Member States should promote the increasing awareness of hardware suppliers by certifying products that meet security baselines and allow DSOs to give priority to such certified products.

- The EC communication "Smart Grids from innovation to deployment" defines smart grids as a "critical infrastructure", which should operate securely and respect privacy of the customer. By complying with the EU's data protection regulations and the EU cyber security policy, DSO could help building trust among their customers.

- A close collaboration with other relevant stakeholders, such as the local national cyber security center (NCSC) CERT, ENISA, Energy regulator, Data protection authority, etc. is crucial in order to prevent, identify and analyse appropriate cyber security measures and manage the threats associated with incidents that involve critical information infrastructures

- The EU and Member States should strive to achieve a cyber security culture. This can be realised only with the support of European and National authorities, and by making cyber security a top priority at the highest level of management, facilitating its inclusion in the company's strategy and enabling proper investment to allow sufficient resources and awareness at all levels.

WG Distribution Customers

Contact:
Giuseppina RONDINELLI, Advisor Distribution -
grondinelli@erurelectric.org

[1] The rising strategic risks of cyberattacks - McKinsey & Company

[2] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union

Table of Contents

1. Cyber Security in the Electricity Sector 1
2. Identified Threats and Challenges 2
   - 2.1 Challenges 2
   - 2.2 Threats 3
3. Current Legal Framework concerning Cyber Secutity, Cyber Crime and Data Protection 4
   - 3.1 Network and Information Security Directive (NIS) 4
   - 3.2 General Data Protection Regulation (GDPR) 5
4. European Initiatives to Enhance Cyber Security 6
5. Enhancing Cyber Security Capabilities 7
   - Prevent and Protect 7
   - Mitigation and Response 8
   - Recovery Process 8
   - Investigate and Improve 9
6. Existing Financing Schemes for Cyber Security and Getting Support 9

1. Cyber Security in the Electricity Sector

Customers' need for electricity is growing as the number of devices connected to the electricity network increases rapidly. The electricity sector is at the beginning of a new era for cyber security. The energy sector is also going through a major digital transformation, with an increase of complexity within its technological environment and an escalation of interconnected equipment.

As the traditional system and business is changing, the energy sector is at one of its most challenging times. Customer driven intiatives such as microgeneration, decentralised power sources and the integration of electric vehicles (EVs) as well as the 2020 and 2030 European-wide climate change objectives will bring new and complex challenges tonetwork operators.

This new paradigm is supported by a complex and highly critical information technology infrastructure, which facilitates the advanced grid and market functionalities, but also increases the exposure of network operators to cyber threats and vulnerabilities, and can present serious risks to customers, businesses and society. These risks can only be mitigated by a well-executed cyber security strategy.

Cyber security can be defined as a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practice, assurance and technologies that can be used to protect the cyber environment, organisation and user's assets. An organisation and its users' relevant assets includes connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cyber security ensures the maintenance of the security properties of the organisation and its users' assets against relevant security risks in the cyber environment. The general security objectives comprise the following: confidentiality, integrity and availability. [3] It is important to stress the fact that cyber security should be looked at not only from a technical point of view, but also from an operational and organisational one. In other words, it is not enough for a company to protect its infrastructure, but also to develop processes and train employees with a cyber security oriented mindset.

Knowing that the electricity grid is arguably one of the most critical infrastructures and many sectors depend upon it, ensuring its resilience should be a top priority for every country. Moreover, as the Informational Technology (digital infrastructure) components and the Operational Technology (physical infrastructure) are increasingly connected to make the grid "smarter", they are also more exposed to attacks via the telecom networks. In the electricity sector, addressing cyber security across countries is crucial as far as the reliability and security of a region's electricity grid are concerned, as an outage may not be limited to just one country.

As the European energy system is becoming more and more interconnected, cyber security should be addressed as a cross-border issue, meaning that cooperation regarding cyber security is needed at European level. This cooperation includes the sharing of information and cyber experts between organisations and countries that are potentially exposed to attacks.

[3] Definition of cyber security from the International Telecommunication Union (ITU) of the United Nations (UN). Sometimes non-repudiation is also added because it is not well captured within the three core concepts.

2. Identified Threats and Challenges

A well-structured European cyber security plan faces multiple challenges and threats that can be summarised as follows:

2.1 Challenges

Besides the impact on the customers, one of the main challenges is the long investment cycles in the energy sector that make technology assessments difficult and led to a time lag between implemented and up-to-date solutions. There is also a need for cross-border coordination, because uncoordinated efforts result in a variety of heterogeneous guidelines, which lead to an inefficient global response to cyber security related incidents.

Furthermore, it is not always clear who is the authority in charge of smart grids cyber security. Although many network operators are tackling effectively this challenge, many others lack the incentive and expertise, and many National Regulatory Authorities (NRAs) lack the mandate to take on this responsibility. However, the EU NIS Directive, which will come into effect in 2018, will change the current paradigm with the creation of national competent authorities responsible for monitoring the application of the Directive at national level. Distribution System Operators (DSOs), as active service operators, will be accountable for security and compliance with the NIS requirements. Therefore, competencies connected with cyber security should be developed in the core business of the DSOs.

Moreover, IT-Security expertise is often outsourced to third parties and vendors, leaving network operators more dependent on external competencies with both benefits and risks. Likewise, IT (Informational Technology) & OT (Operational Technology) environments have mismatching life-cycles and diverging practices in terms of design, qualification and maintenance, which can lead to a different approach regarding the security of each technology, creating gaps that can be maliciously exploited.

Another challenge is the increased use of commercial ‘off the shelf’ products, to keep up with smart grid development. This leads to a dependence on the reliability of hardware suppliers with regards to cyber security which usually is insufficient. On the other hand, ‘tailor made’ solutions are also not necessarily the optimal way out, as they can lead to some financial and technical inefficiencies (tailor made solutions are typically more expensive to develop, upgrade and maintain when compared to COTS (cost off –the shelf) that are commercially available for a high number of customers and tend to have longer design-to-production cycles that generally uncover design defects or vulnerabilities early).

Currently, the DSOs are responsible for setting and controlling the security baseline. National authorities should set security baselines that equipment and service providers have to follow and provide security certifications for products that DSOs use on their networks or for products that could be used by third party companies (eg. energy suppliers, ESCO’s, aggregators) on the customer premises (Home Area Network). Also, customers should have a defined level of security in every device that they use, no matter how they are connected with network. This could be done by setting up baseline security certifications in every Member State and ensuring their mutual recognition. This would also be a step towards the opening of the security market in Europe. The fast pace of smart grid development is a challenge also due to the highly heterogeneous hardware and software that is used throughout the grid, which adds even more complexity the current intricate equation.

The scale of smart grid deployments is also an obstacle to the implementation of security controls. Since many smart meters and data concentrators are being deployed (millions), the implementation of security requirements might represent an unacceptable cost overhead for the (sometimes) fragile business cases. The amount of meters, as well as any other HAN connected devices, also represent a challenge in respect of the maintenance and operation costs. For instance, if a non-remote update is required, it is a complex and costly problem to locally upgrade them. Moreover, considering the long life cycle of this equipment, it is hard to believe that they can continuously be enhanced and updated to endure and defend against the future security threats without any associated hardware upgrades.

Having suitable cyber security analytics is also a key aspect in addressing fast evolving threats. In the future, malware mutations and the complexity of the Advanced Persistent Threats (APT) call for different approaches. Cyber security analytics represent a more dynamic effort on cyber defence, by performing real-time behaviour analytics and anomaly detection.

However, perhaps the biggest challenge of all is to perform a deep organisational transformation. Cyber security is not a mere technical subject. On the contrary, the company should develop its own cyber security culture. This implies empowerment, commitment and most of all a mindset change for all employees.

2.2 Threats

An electric company's digital infrastructure comprises different components that are exposed to threats:

- BDC (Billing and Debt Collection), systems with personal information of the customers.
- SCADA (Supervisory Control And Data Acquisition) refers to centralised systems which monitor and control entire sites or complexes of systems spread out over large areas (anything from an industrial plant to a national utility network);
- PLC (Programmable logic controller) is a digital computer and a subsystem of SCADA. It is used for automation of typically industrial electromechanical processes, such as control of machinery on factory assembly lines, protection relays, fault recorders, etc);
- EMS (Energy Management Systems) or DMS(Distribution Management systems) are systems of computer-aided tools used by operators of electric utility grids to monitor, control and optimize the performance of the generation , transmission system and/or distribution electrical system;
- CPS (Cyber Physical System) is a mechanism controlled or monitored by computer-based algorithms;
- PLC (Power Line Communication) and the Public Cellular Network are the most commonly used in the implementation of smart meters;

With the growing interdependency between systems and telecom networks, there are many vulnerabilities that can be exploited by criminals.[4]An example would be the incident that happened in Ukraine on the 23rd of December 2015, when at least eight energy distribution companies were attacked. The attack resulted in power failures that affected 225,000 customers. Although the attack was not technically sophisticated, it took months of planning, which shows the high level of knowledge the hackers have about the network' operational systems.[5]

In such cases, the goals of the attacker are usually the same: to damage crucial systems, to gain superiority, to intimidate the opponent from an economic point of view causing loss of lives.

For the energy sector, a blackout can have severe direct and indirect impacts Examples of direct impacts include business shutdowns, food spoilage, damage to electronic data and equipment, the inability to operate life-support systems in hospitals and households and the loss of functionality of other critical infrastructure such as wastewater treatment plants. Indirect impacts include property losses resulting from arson and looting, overtime payments to emergency management personnel and potential increases in insurance rates.[6]

[4] The cost of incidents affecting CIIs
[5] Everything We Know About Ukraine's Power Plant Hack - Wired
[6] Book - Physical vulnerability of electric systems to natural disasters and sabotage.

3. Current Legal Framework concerning Cyber Secutity, Cyber Crime and Data Protection

Currently, the EU is working on a number of fronts to ensure cyber security in Europe, from providing the delivery of improved internet for children, to implementing the international cooperation on cyber security and cybercrime.[7]

3.1 Network and Information Security Directive (NIS)

In 2013, the European Commission (EC) put forward a proposal for a Directive concerning measures to ensure a high common level of network and information security across the EU.

In July 2016, two years later, the European Parliament and Council agreed on the text and the NIS was adopted on 6 July 2016. The Directive entered into force in August 2016. Member States will have 21 months to transpose the Directive into their national laws and 6 months more to identify operators of essential services.

The NIS Directive provides legal measures to increase the overall level of cyber security throughout the EU and its main objectives are:

- Increasing the cyber security capabilities in the Member States, by establishing local authorities responsible for Network and Information Security. Therefore, each country will have its own authority that is responsible for creating a national strategy to adopt the NIS Directive;

- Enhancing cooperation on cyber security among the Member States, inside a network that allows an efficient coordination, including coordinated information exchanging, as well as detection and incident response at EU level;

- Ensuring a high level of risk management practice in key sectors (such as energy, transport, banking and health). These include information sharing between public and private sectors, the responsibility of each company and institution with critical infrastructures to report any incident that affects its critical systems and business continuity. However it must be noted that the total amount of information, its storage and communication flows must be protected by confidentiality and privacy reasons, since they are a source of revealing vulnerabilities and risks in one or more of the operators' IT infrastructure.

The NIS Directive calls the energy sector as one “key sector” and refers to distribution system operators (DSOs) as “operators of essential service”. Therefore, DSOs should ensure the security of networks and systems, which they use. Moreover, it states that the operators of essential services have the responsibility of ensuring that the Directive is applied correctly. [8]

The need for a Directive, that standardises the cyber security requirements and measures that Member States should adopt, is supported by the fact that in 2015 only 19 of the 28 Member States have a comprehensive cyber security strategies in place, while eight have not declared any such framework at all. Even in the case of countries with adopted cyber security strategies, the quality is variable, many remaining vague and high-level, lacking a clear implementation plan.[9]

It is important that EU Member States recognise cyber security as an important subject to address and should work towards cyber resilience, with particular focus on protecting the country’s critical infrastructures. The first attempt to address this matter was Directive 114/2008, which obliged Member States to identify a

[7] https://ec.europa.eu/digital-single-market/en/cyber security
[8] Network and Information Security Directive, 26
[9] EU Cyber security Dashboard - A Path to a Secure European Cyberspace

"European Critical Infrastructure" (ECI). Being identified as a European Critical Infrastructure brings about the eligibility for special support. This Directive, alongside the NIS Directive will increase attention and support of cyber security issues in the electricity grid.

Another EU initiative regarding the critical infrastructures is the Critical Information Infrastructure Protection (CIIP) action plan, in which the EC states that purely national approaches are not enough and that it intends to set up a network of well-functioning CERTs by 2012. The main achievements of this action plan were: the establishment of the European Forum for Member States and of the European Public-Private Partnership for Resilience; carrying out of pan-European exercises (Cyber Europe 2010 and 2012); adoption by ENISA of a minimum set of baseline capabilities and services and related policy recommendations for National/Governmental Computer Emergency Response Teams (CERTs) to function effectively.

However, this action plan still lacks the important proposals of the NIS Directive regarding the obligation of Member States to put in place a minimum level of capabilities at national level and to cooperate cross-border.

3.2 General Data Protection Regulation (GDPR)

An important EC initiative on data protection is enshirned in the The General Data Protection Regulation (GDPR). The GDPR was ratified by mid 2016 and immediately became law. Member states now have a two year implementation period. Enforcement will commence by mid 2018 at the latest.

This Regulation is designed to enable individuals to better control their personal data and addresses to any particular industry or organisation. It generally refers to how companies and, in our context network operators, handle, process and protect personal data. Processes from collection, processing, retention and deletion will have to be revised so that they are compliant under the stricter data protection rules, and internal governance processes will have to change accordingly.

"Personal data" is defined in both the NIS Directive and the GDPR as any information relating to an person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. So in many cases online identifiers including IP address, cookies and so forth will now be regarded as personal data if they can be (or are capable of being) without undue effort linked back to the data subject The Regulation clearly addresses the tasks, rights and responsibilities of and the interactions between the following roles: Data subject, Controller, Processor, Recipient of data (whether a third party or not), Data protection officer, Supervisory authority.

Also, according to the GDPR, National Regulators will now have authority to issue stringent fines[10], penalties[11] and compensatory damages for infringements. Administrative fines alone for noncompliance with certain GDPR provisions can be up to 20 million Euros or 2% percent of a company's total worldwide annual revenues for violations of record-keeping, security, breach notification, and privacy impact assessment obligations.

Once the GDPR is in effect, the current Data Protection Directive 95/46/EC is repealed. As companies and , among others, network operators begin the process of moving to compliance with the new requirements, Member States should take into account the impact on national legislation that implements the Directive.

Being this Regulation applicable to any organisation that holds and processes personal data (for example smart meter data) it particurarly affects DSOs given the increasing number of smart meter deployed across Europe, the size of prosumers connected to DSO networks and the availability of connected devices (in the home, office, etc) that represent potential access points for hackers and cyber terrorists.

[10] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Article 83
[11] http://eur-lex.europa.eu/eli/reg/2016/679/oj, Article 84

4. European Initiatives to Enhance Cyber Security

Despite cyber security being a recent subject, a number of initiatives have already been conducted by Member States in order to enhance the country's ability to face any attack. Member States need to learn about best practice from other sectors or other world regions that deal with highly sensitive information or are subject to cyberattacks on a regular basis.

For example:

- In Denmark, there is a close exchange of data between the transmission system operator (TSO), DSOs, generators and retailers via a data hub. Energinet.dk (TSO) is responsible for data security in relation to information exchange in the electricity market, but it has outsourced the security service to a third party;

- In Norway, companies are obliged to report major incidents (including cyber security incidents) to the national authority NVE. Apart from that, in 2014 Norway has set up "KraftCERT" (see https://www.kraftcert.no/english/index.html);

- In Austria, there is a public-private cooperation in order to set up (voluntary) national security and safety standards for the power industry, carry out a risk assessment and develop an action plan to tackle these risks;

- In France, companies are about to be obliged [12]to report large cyber security incidents to the national cyber authority, ANSSI. There is also a CSPN[13] certification for black box testing of product security level. However, there is a lack of mutual recognition with other Member States: no market for suppliers, therefore no incentive for certification. That is why it has been mainly used only by Small and Medium Enterprises (SMEs) so far;

- In Sweden, there is a long tradition of cooperation between the energy sector and the responsible authorities regarding all security matters. A common security website for the energy sector (www.energisakerhetsportalen.se) has been developed where all relevant information is gathered;
- In Portugal, the National Cyber security Center (CNCS, see http://www.cncs.gov.pt/pagina-inicial/index.html), part of the National Security Authority, ensures effective crisis management, coordinates the operational response to cyberattacks, develops national synergies and enhance international cooperation in this field. It has been developing a number of initiatives closely related to the energy sector;

- In Germany, the national IT-Security Act came into force in June 2015. Since May 2016, operators of critical infrastructures in the energy sector are obliged to report network and information security incidents that may have a disruptive effect on the provision of their service. In addition to that, all DSOs and TSOs need to fulfill a catalogue of IT-security measures and implement an Information Security Management System (ISMS) compliant with ISO/IEC 27001. Electricity generation plants that have been identified as critical infrastructures will need to fulfill a different catalogue of IT-security measures that is currently being drafted by the national regulatory authority."

[12] In France a decree has been published to force some companies to declare security incidents to the French cybersecurity authority, but the details are left to a regulation that will enter into force only during year 2017.
[13] "Certification de Sécurité de Premier Niveau" in French, which means "basic cyber security certification"

At EU level, there are also a number of possible examples of "prevent and protect" projects and initiatives, with the purpose of creating a more cyber secure EU, in particular projects that deal with cyber security in the electricity grids, for example:

- SESAME project, that developed a Decision Support System (DSS) for the protection of the European power transmission, distribution and generation system (see *https://www.sesame-project.eu/*);

- C-DAX project, that proposed a Cyber-secure Data and Control Cloud for future power distribution networks as an integrated communication and information infrastructure. C-DAX exploits the properties of novel, information-centric networking (ICN) architectures that are more secure, resilient, scalable and flexible than conventional information systems (see *http://www.cdax.eu/*);

- SEGRID project, whose main objective is to enhance the protection of smart grids against cyber attacks. The project tackles this subject by applying a risk management analysis approach to a number of smart grid use cases (the SEGRID use cases), which will define security requirements and determine gaps in current security technologies, standards and regulations. The identified gaps and the analysis itself will give input to the enhancement of risk assessment methodologies and the development and testing of novel security measures for smart grids (see *http://www.segrid.eu/*);

- SPARKS project, which aims to provide innovative solutions in a number of ways, including approaches to risk assessment and reference architectures for secure smart grids. The project will make recommendations regarding the future direction of smart grid security standards. Furthermore, the project also investigates key smart grid technologies, such as the use of big data for security analytics in smart grids, and novel hardware-supported approaches for smart meter (gateway) authentication (see *https://www.project-sparks.eu/*);

- EE-ISAC information sharing network, which enables an open and honest conversation between the public and private sector, providing benefits to all participants (see http://www.ee-isac.eu/).

5. Enhancing Cyber Security Capabilities

In order to protect our customers and have a better and faster response to cyber-attack, all companies and in particular network operators should have a defined process about how to act. It should be noted that hackers broke into the Ukrainian networks nine months before the outage and five out of the eight attacked power distribution companies have been able to detect and mitigate the incident before it had effects on the main system. Hence, intrusion detection systems and processes are the cornerstone of cyber security when it comes to network operators. Such processes consist of the following stages:

Prevent and Protect

Cyber security incident prevention and protection must address threemain topics, (1) the number of customers expected to be affected, (2) the implementation of controls that allow a mitigation of the existent vulnerabilities and (3) the enablement of an accurate and efficient ability to detect and respond to incidents.

Regarding incident prevention and the mitigation of existent vulnerabilities, some key elements should be taken into consideration in order to allow a better response afterwards. These elements include:

- Suitable cyber security policies;
- Incident response plan;
- Communication plan;
- Incident Response Team;
- Mechanisms that allow an in depth protection;
- Training and raising awareness among employees.

Usually, incident response methodologies stress the importance of preparation, not only in establishing incident response ability, but also in incident prevention, by ensuring that systems, networks and applications have a suitable cyber security level regarding each organization's risk management. If cyber security implementations are not suitable, incidents can not only occur, but also create an overload on the company's resources response ability, resulting in greater damage and slow recovery. To prevent these situations from happening, organisations should have the appropriate resources, as well as the appropriate training, which implies an increase in awareness of the company's policies and procedures regarding networks, systems and applications.

Regarding the protection of the company, there are also some key elements that should be taken into consideration, that include:

- Security testing;
- Incident monitoring systems;
- Backups;
- Cyber intelligence for attack prediction;
- Audits;
- Attacker profiling;
- Spare workstations, servers and network equipment;
- Comprehensive risk assessment;
- Forensics capabilities (software, teams and procedures).

Mitigation and Response

When responding to incidents, there are three main factors that should be taken into consideration, which will affect the incident's mitigation and response process. First, incidents can be detected in many different ways, with different levels of detail. Second, the amount of data that may contain evidence of an incident is usually very large, particularly in a large company/organization. Lastly, technical knowledge and wide experience are essential to perform a suitable and efficient analysis of incident related data.
If an incident occurs, the first step is to detect which systems are affected, where is the origin of the attack and understand the incident's anatomy (i.e., tools that are being used, vulnerabilities that are being exploited, etc.). The initial analysis of the incident should provide enough information to start the mitigation and response process.

Limiting as much as possible the impact of the incident is the top priority of the mitigation process (but with a necessary trade off with IOC[14] and evidence collection, in order to be sure of the effective mitigation of the incident and be able to engage legal response and feedback). The required measures to an effective mitigation may vary with the infrastructure and technology that has been affected. They can vary from simple network segment isolation to a shutdown of several critical servers.

Identifying all damaged systems is the first step of the response process, to allow better decisions regarding necessary actions, such as malware deletion, user's accounts deactivation, etc. Typically, these actions require the assistance of anti-virus tools, spyware removal packages.

While analyzing and responding to the incident, it is required (to comply with the NIS Directive) to inform the local CERT. Once the criticality is evaluated, the response and notification procedures should be adapted accordingly. The existence of a Cyber Security Operation Center is also recommanded to constantly monitor the critical infrastructures.

Recovery Process

The recovery process should start with the restoration of all the affected systems, by first trying them in a controlled environment, to make sure that no further incident will occur when they are connected again to

[14] Indicator of Compromise

the company network. Furthermore, it is also crucial to test and monitor every affected system when they are connected again to the network, considering that the danger they might represent is still higher than average.

There are some important actions/decisions required during this process, such as scheduling the system shutdowns and restarts, how to verify if the affected systems are safe and functional, how long these systems should remain under a tight monitoring and which tools are suited to perform such monitoring. The system should only be reconnected to the SCADA network after being considered as functional and without any virus.

Investigate and Improve

During the investigation phase, all the documentation that has been created during the incident analysis and response should be aggregated, as well as any additional information that is still missing or that is considered relevant. This information should all be studied in order to avoid failures on the company's cyber security policies and procedures.

At the end of the incident, it may be possible to identify all the systems that were affected, where the incident started, why it happened, when it happened and when it was solved. It should also be possible to understand the extent of the impact and which measures were taken in order to fully eliminate all traces of the incident.

All the reports generated with the above mentioned information are relevant not only for legal purposes, but also for training and information sharing with other relevant European partners and stakeholders, such as the local national cyber security centre (NCSC) CERT, ENISA, Energy regulator, data protection authority, etc. All this combined enables organisations to prevent and be better prepared for future incidents. Generally, national and international flows of information and best practice among energy firms play a key role in cyber security.

6. Existing Financing Schemes for Cyber Security and Getting Support

In most of the Member States, DSOs as regulated entities need national legislation that enables them to have access to sufficient financial means to ensure a high level of cyber security[15]. Therefore, Regulations and Directives, in particular from the EU, such as the NIS Directive, are crucial because they leverage the inclusion and development of the subject in every Member State agenda, ensuring a high common level of cyber security in the EU. Also, all companies/organisations that deal with critical infrastructures shall adopt risk management practices and report major incidents to the national authorities.

For the DSOs to get support from other players in the market, the existence of mutual cooperation regarding intelligence and workforce sharing is crucial. This cooperation can either be by each company's own initiative or by joining information sharing groups as the European Energy - Information Sharing & Analysis Centre (EE-ISAC). It is important to learn not only from each other's cyber security policies and efforts to secure the network, but also from incidents, errors and failures. This sharing of information should also be made between DSOs and the local security authorities, as specified in the NIS Directive.

In order to ease the work of DSOs architects and to provoke rapid awareness from service and equipment providers, certification schemes have to be developed at a pan-European level. Currently, the responsibility of setting and controlling the security baseline is left only to DSOs. National authorities should set security baselines that suppliers have to follow and to provide security certifications for products that DSOs could use on their networks. A way to do that could be through setting up baseline security certifications in every Member State and ensuring their mutual recognition. This would also be a step towards the opening of the security market in Europe.

[15] It should be noted that in the UK Ofgem provides no regulated funding for cyber security investment.

EURELECTRIC pursues in all its activities the application of the following sustainable development values:

Economic Development

- Growth, added-value, efficiency

Environmental Leadership

- Commitment, innovation, pro-activeness

Social Responsibility

- Transparency, ethics, accountability

Union of the Electricity Industry - EURELECTRIC aisbl
Boulevard de l'Impératrice, 66 - bte 2
B - 1000 Brussels • Belgium
Tel: + 32 2 515 10 00 • Fax: + 32 2 515 10 10
VAT: BE 0462 679 112 • www.eurelectric.org
EU Transparency Register number: 4271427696-87