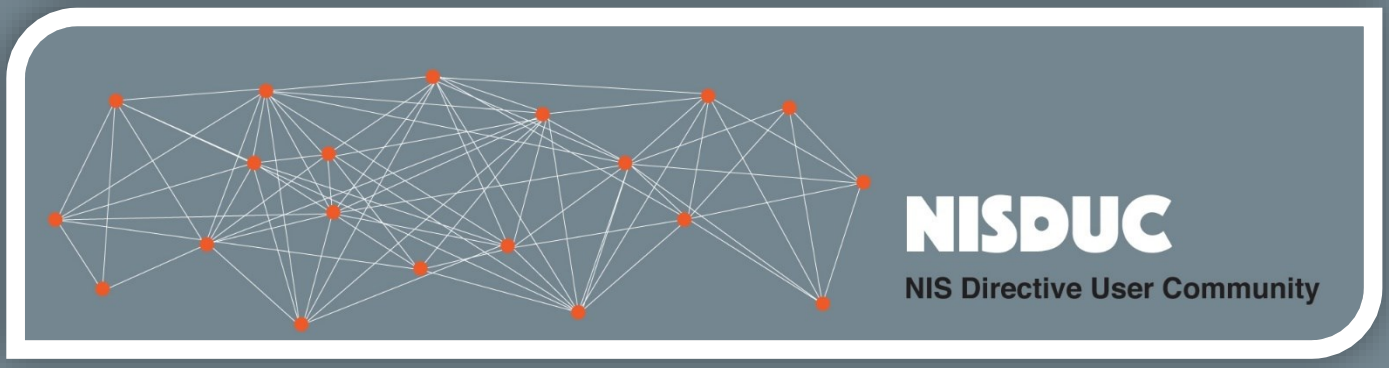

D3.3: NISDUC Lessons learnt – vol.3

Co-financed by the European Union
Connecting Europe Facility

Project acronym	NISDUC
Project title	NIS Directive User Community
Start date of the project	01/09/2020
Duration	36 months
Funding instrument	Connecting Europe Facility: Telecom (CEF Telecom)
Call for proposals	CEF-TC-2019-2 – Cybersecurity
Objective	Objective 4: Trans-European cooperation for effective joint cybersecurity operations and to build mutual trust/confidence
Agreement number	INEA/CEF/ICT/A2019/2072562
Action No	2019-EU-IA-0129

Deliverable type	Report
Deliverable reference number	D3.3 / V1.0
Activity contributing to the deliverable	Activity 3: Monitoring on the practices and experiences of the implementation of the NIS Directive
Due date	30/04/2023
Dissemination level	Public
Revision	V1.0

Contributors (ordered according to beneficiary numbers and alphabetical order of first names)

Hervé Cholez, Jocelyn Aubert, Nicolas Mayer, Jean-Sébastien Sottet (**LIST**)

Guy Mahowald, Pascal Bertrand, Sascha Maurer, Sheila Becker (**ILR**)

Albert Jorissen, Nicolas Lempereur, Philippe Faccinetto, Pierre-François Vandenhaute, Rudi Smet, Tim Masy (**BIPT-IBPT**)

Alexandre Dulaunoy, Gérard Wagener (**CIRCL.LU**)

Reviewers

Caroline Breure (**CCB**)

Disclaimer

Table of contents

Lessons learnt from a collaborative approach involving Operators of Essential Services (OES), the National Competent Authority (NCA) and the Single Point of Contact (SPOC)

This section suggests best practices and experiences to implement the NIS Directive, based on a collaborative approach of regulated entities (Operators of Essential Services (OES)), regulatory authorities (National Competent Authority (NCA) and the Single Point of Contact (SPOC)).
These practices refer to studies set up by, for Luxembourg, the **Institut Luxembourgeois de Régulation (ILR)**, the NIS identified SPOC, the NCA for the DSPs and for OES (except for banking and the financial market infrastructure), and, for Belgium, the **Belgian Institute for Postal services and Telecommunications (BIPT)**, the NIS sectoral authority for Digital Infrastructures in Belgium, both assisted by the **Luxembourg Institute of Science and Technology (LIST)**, a mission-driven Research and Technology Organization that develops advanced technologies and delivers innovative products and services to industry and society.

Towards a national systemic analysis of the cybersecurity ecosystem

Nowadays, enterprises from different sectors are strongly interconnected and need to interact continuously to survive. In this context, the occurrence of an event (e.g., system failure) in one sector may lead to a serious risk in another. This is particularly the case in the NIS Directive [1] context with essential and important entities. In addition, NIS 2 Directive [2] adds a specific focus on supply chain security compared to the first NIS Directive. Indeed, one of the measures provided addresses supply chain security by requiring security-related aspects to be included, concerning the relationships between each entity and its direct suppliers or service providers.

Challenges of supply chain security

In the regulatory context currently established in Luxembourg and Belgium, risks are assessed individually by each organization for their own activities. No link is established between the risk management results of interacting organizations. However, services offered by OES are generally composed of sub-services commonly provided by different service operators. Consequently, it is currently not possible for the NCA to be aware of intra-sectoral or cross-sectoral impacts of risks. These impacts may even be worse than the impact on single company only.

Moreover, it is not possible for the NCA to be aware of the actual risks harming the end-user (i.e., to have a customer-centric risk approach), which is by essence what is targeted by the NIS Directive [1] and other regulations (e.g., the EECC [3]). The aim of the NIS Directive is indeed to try to minimize as much as possible risks taken by the citizens related to the use of essential services, and avoid critical situations such as, e.g., the incapacity to use ventilation support machines in a hospital due to a power outage.

It is thus necessary to have a more holistic view to perform risk management for the whole supply chain. However, a key constraint related to this issue is that confidentiality must be kept for the risk management data between supplier/customer. The main question is thus: how to reconcile individual security risk management established by OES to identify and analyse systemic risks coming from dependencies between OES?

The proposed approach is composed of two complementary layers which will be detailed in the next sections:

Layer 1: **Ecosystem modelling and systemic indicators**

A graph-based framework dedicated to security and analysis of complex ecosystems (e.g., NIS essential services providers at a country level).

Layer 2: **Risk cascading and ecosystem risk management**

A systemic risk management approach allowing risk cascading between dependent organisations and large-scale incident simulation.

First insights of such a systemic approach to security risk management have been elaborated in a research paper published in 2020 [4] and will be extended here.

Ecosystem modelling and systemic indicators

The objective of this layer is to develop an analysis framework for the OES ecosystem, being highly interdependent. The goal is to analyse the ecosystem as a whole and simulate possible impacts on the security of the supply chain composed by several OES, all of them needed to provide services to the end users.

To do so, we have developed a graph-based framework dedicated to the analysis of complex ecosystems (e.g., NIS essential services providers at a country level). The main features are ecosystem modelling, generation of KPI related to security and risks, and impact assessment (at the service level). The framework aims at being interoperable with other applications and analysis tools of the NCA, e.g., considering each individual risk reports or notified incidents. The target user is the NCA who is the only actor with access permissions to the needed data.

Scope and questions addressed

The scope of this work is focused on 1) establishing an ecosystem composed of OES and their inter-dependencies in terms of services and 2) performing analyses based on the dependencies and the ecosystem configuration. It is worth noting that risk-based analyses are out of the scope of this layer but addressed in the second one. Here, the focus is put on systemic analysis performed at the service and organisation level, and not at the infrastructure and risk level. The questions we want to answer with our approach are the following:

Focus on one specific service or organization:

- What is the **criticality of an organisation** based on the dependencies it has?
- What is the **criticality of a service of a given organisation** based on the dependencies it has?
- How **vulnerable to external outage is a given organization** based on the dependencies it has?
- How **vulnerable to external outage is a service of a given organization** based on the dependencies it has?

Ranking and focus on the most critical and the most vulnerable services or organisations:

- What are the **most critical organisations** for the ecosystem?
- What are the **most critical services** for the ecosystem?
- What are the **most vulnerable organisations** of the ecosystem?
- What are the **most vulnerable services** of the ecosystem?

Focus on one sector / sub-sector:

- What are the **dependencies within** a sector/sub-sector?
- What are the **dependencies between** 2 specific sectors/sub-sectors?

Design of the ecosystem

First, the list of OES in scope is established. For each OES the service(s) provided, it specifies its type and its sector/sub-sector. Next, the service dependencies are gathered at the level of each OES. They consist of the list of the essential services on which the organization depends on, including the name of the service provider and the list of essential services it provides to other OES with the name of the service customers. If the dependency is rooted in a foreign organisation, it will be indicated as well.

The ecosystem modelling language is based on the following concepts:

> **Organization**: one specific company or administration. Within the frame of the NIS Directive: an OES (or a DSP).
>
> **Service**: a service delivered by an organization. Within the frame of the NIS Directive: an essential service provided by an OES.
>
> **Sector/sub-sector**: the sector of activity of the organization. Within the frame of the NIS directive: the NIS sector/sub-sector as depicted in Annex II of the NIS Directive [1] about the types of entities.
>
> **Dependencies**: the dependencies to services provided by other organizations / the services provided to other organizations.
>
> **Customers**: the final users/customers (national citizens) of one or several service(s).

The structure of the model, to represent an ecosystem, is a graph. It is adapted as follow: OES are nodes and services are relations between these nodes. Based on the questions we want to answer, requests are generated and applied on the ecosystem, leading to specific views of the graph (or of a subset of it). Such views are defined considering only a selection (i.e., result of a query), a combination or a transformation of concepts pertaining to the initial ecosystem model. Views can be a filter, for instance, regarding a given sector where the sub-graph displays OES of the sector and its related services. Additional data can also be displayed such as the number of impacted users.

Examples

A first implementation has been performed with Neo4j as the graph database management system and Bloom as the framework for graph visualisation, both being integrated in the Neo4J Platform[1].

Figure 1 represents the result of the request: "*What is the place of the energy provider named EastElec in the ecosystem?*". As a result, we can see the *EastElec* company and all the other OES with which it has interdependencies (until level N). The following information are automatically extracted from the graph represented in Figure 1:

- 42 outgoing dependencies (total)
- 23 ingoing dependencies (total)
- 1 service supplied by this organization
- 12 services used by this organisation (total)
- 342.800 final users depending on the provided service

[1] https://neo4j.com/

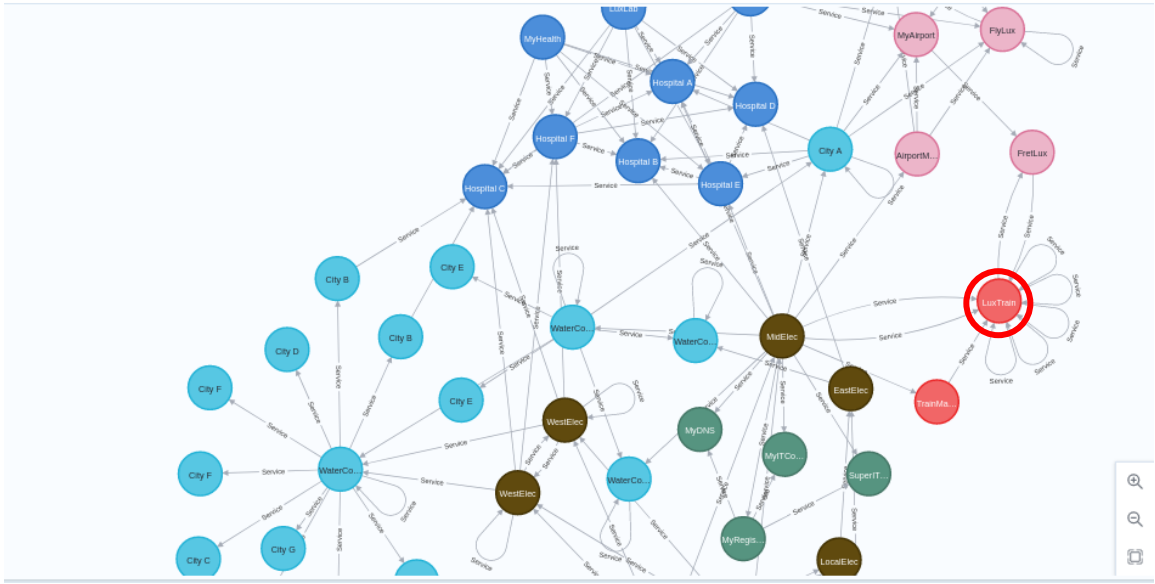

Figure 1. Example of request related to one specific organisation

Figure 2 is a second example which is the result of the request: "*How vulnerable is Hospital A?*". The resulting graph shows *Hospital A* and all its incoming dependencies. The following additional information are provided, coming from the reports of the concerned OES:

- Average risk level of the necessary organizations/services: 7
- Number of inherited unacceptable risks: 15
- Number of incidents over the past year in the necessary organizations/services: 3

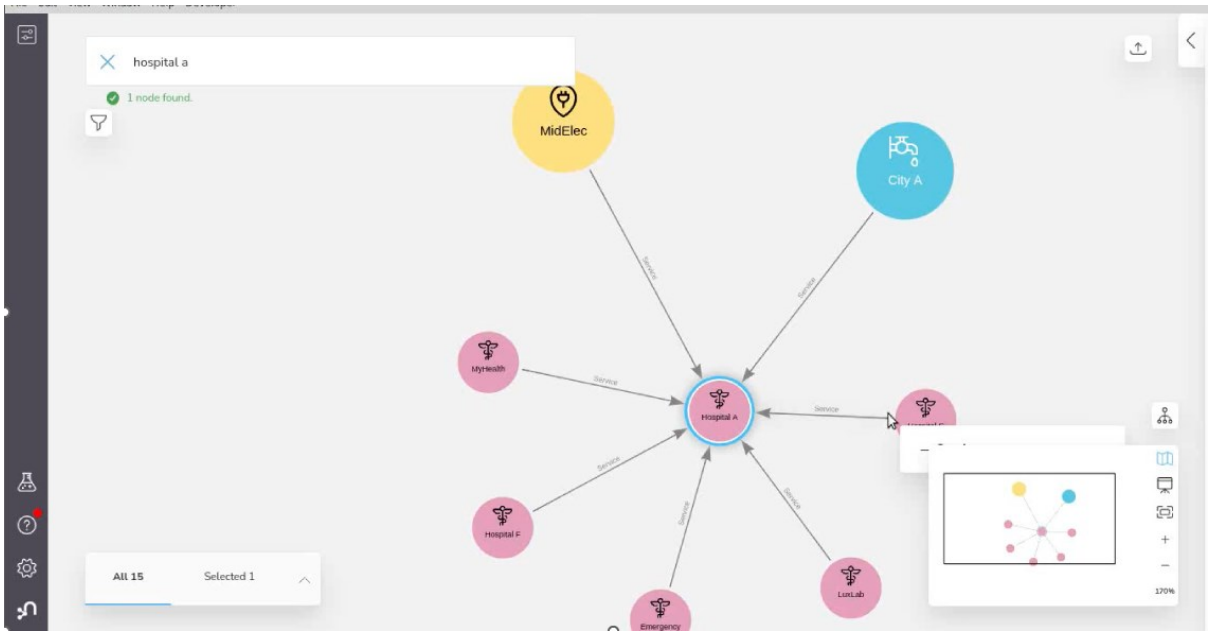

Figure 2. Example of request related to one specific organisation and its risk-related data

Finally, Figure 3 displays the graph associated to the request: "*What are the dependencies of the health sector on the energy sector?*".

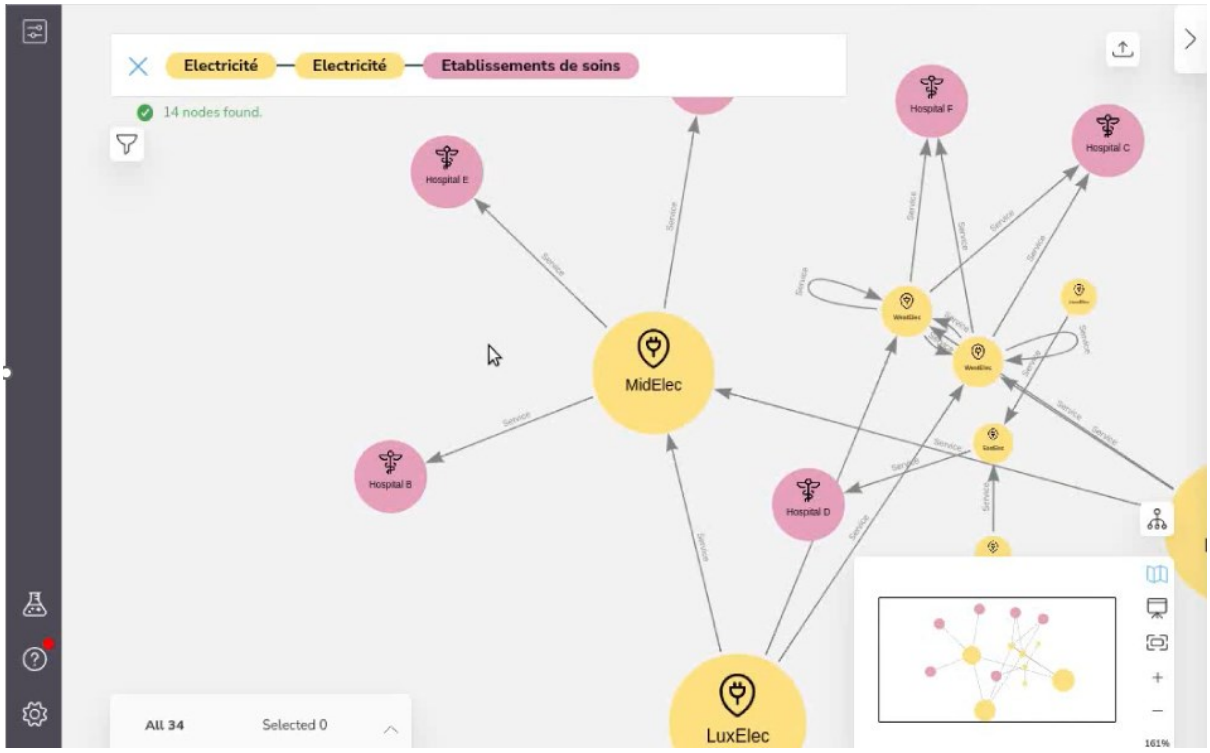

Figure 3. Example of request related to the dependencies between (sub-) sectors

We can conclude from this request that in the health sector, the electricity market is shared between the following actors:

- MidElec: 50%
- WestElec: 30%
- EastElec: 20%

Cascading risks and risk management of the ecosystem

The objective of this layer is to propose a systemic risk management approach considering the OES' individual risks and their cascading risks on dependent OES. Our objective is to cope with this crucial issue: to be able to assess risks at the level of the network of companies providing essential services to the end-user. It is thus necessary to connect the different individual risk assessments to identify the risks taken at the different levels of the supply chain (e.g., cumulative consequences), as well as the risks harming the end-users of the service.

The primary purpose of the developed approach is to allow reconciling individual security risk management reports established by OES to identify systemic risks, coming from dependencies between OES. This approach is to be used by the NCA. They are the only actors having a complete view and a full access to the information of the ecosystem. An example of such dependencies can be, e.g., a hospital depending on telecommunications services provided by a Telecommunications Service Provider, itself depending on an energy provider. In the rest of this section, OES providing services to other OES are named '*service providers*' and OES using services provided by other OES to provide their own services are named '*service consumers*' (an individual operator could play both roles, as the Telecommunications Service Provider in the previous example who provides services to the hospital and uses services from the energy provider).

In this context, the NCA has several Business Questions (BQ) it wants to answer:

- BQ1: What are the new/emerging risks coming from propagation of risks due to dependencies between OES?
- BQ2: Are the risk-related assumptions done by service consumers, especially likelihood of risks, sound regarding their actual assessment by service providers?
- BQ3: What are the most critical OES / services / assets in the ecosystem of the sector from a risk perspective?

To answer the previous business questions, the following Research Questions (RQ) need to be answered:

- RQ1: How to model dependencies between OES at the level of services / at the infrastructure level? (contributing to all BQ)
- RQ2: How to cascade risks of OES being service providers to risks on service consumers? (specifically contributing to BQ1)
- RQ3: How to cascade risk assessments of the service providers to (update of) risk assessments on service consumers, to reconcile the data? (specifically contributing to BQ2)
- RQ4: How to value the criticality of OES / services / assets based on security risks? (specifically contributing to BQ3)

Our proposal is a method composed of three sequential steps.

Step 1: **Dependency modelling**. The dependency modelling is based on dependency statements established by the OES. At the end of this step, a model for the ecosystem at stake is available.

Step 2: **Risk propagation and systemic risk analysis**. For each risk targeting an asset / function / service used by a service consumer, the resulting risk generated at the level of the service consumer is identified and its level analysed.

Step 3: **Systemic risk evaluation**. With the help of the dependency model and the associated propagation of risks, the NCA will be able to evaluate systemic risks at two different levels. First, a consolidation at the risk identification level will be possible, i.e., the NCA will verify if the threats generated by the propagation of risks have all been identified and addressed by the related OES in their report. This task allows answering BQ1. Second, a consolidation at the risk analysis level will be done, i.e., the competent authority would verify if the likelihoods associated to the propagated threats are relevant regarding the risk levels of the original risks of the provider. This task allows answering BQ2. At the opposite of Step 1 and 2, this step is not further detailed, because the detailed approach is dependent on the policy-making strategy of the NCA.

Dependency modelling

To build a model of the ecosystem, which is the goal of this task, a sectoral reference model was established as a specialisation of an enterprise architecture model and designed in the ArchiMate language [5]. We reuse and adapt the ArchiMate language to use it as a reference architecture, selecting a specific subset of the language that is relevant for risk management purpose.

This reference architecture model is presented in Figure 4. It describes all the elements from the assessed OES that are used to perform security risk management. Note that the semantic of this model is partially different from the original semantic of ArchiMate as we focus on information system security concern. This semantic has been rationalised in previous work [6].

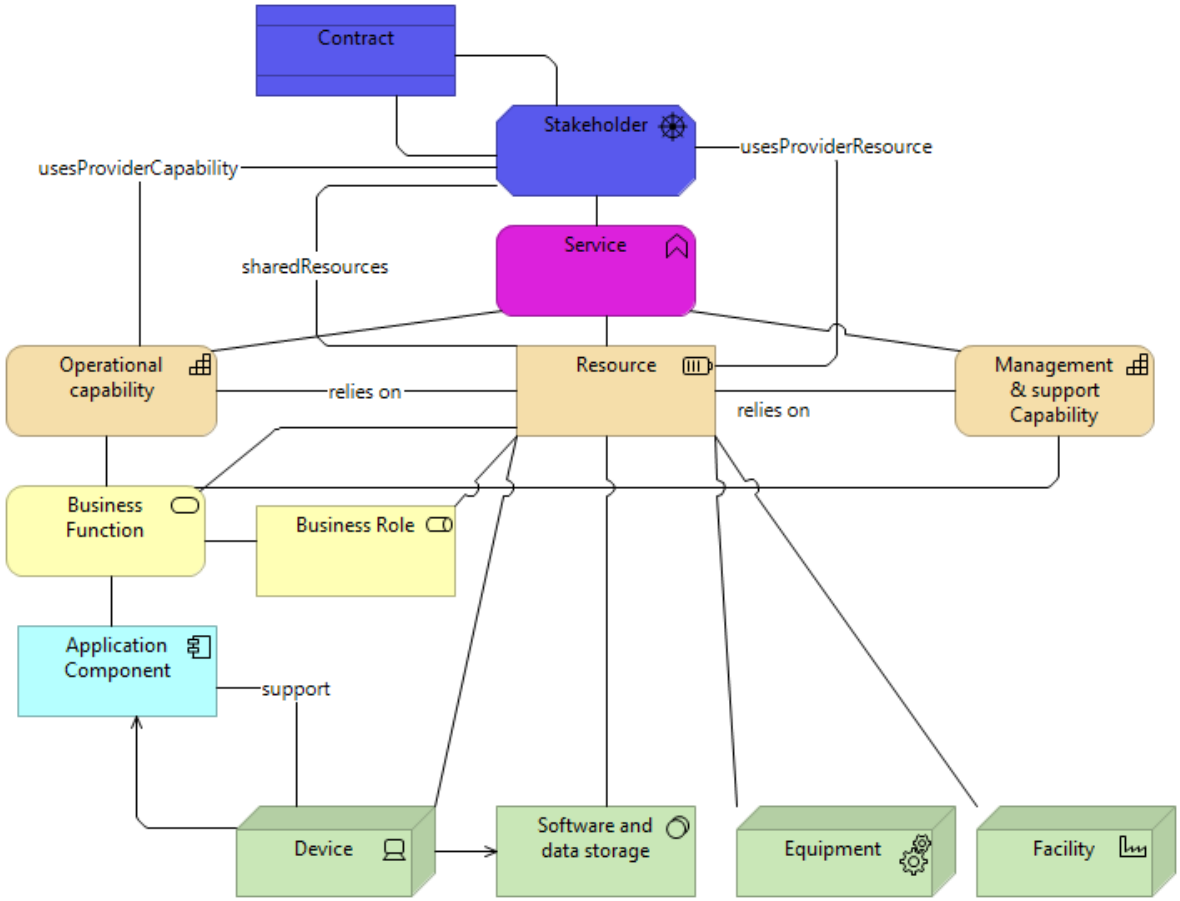

Figure 4. Reference Architecture for OES used for security risk management

The root model element is the S*takeholder* (i.e., representing the OES). The stakeholders provide main services represented by the *Service* model element. Services are described at a high level of abstraction. They are basically the regulated services provided by OES in accordance with the NIS Directive [1]. To work properly, a *Service* relies on *Operational Capability* and *Management & support Capability* as well as the physical and software *Resource*. Those capabilities (operational and management/support) can be decomposed into *Business Function*. For instance, *Management & support Capability* can be composed of H.R. management as a Business Function. *Operational capability* depicts the main functional processes necessary to render the service. An *Operational Capability* can be decomposed into multiple business functions. For instance, in the health sector, blood transfusion (seen here as an operational capability) is composed of several business functions such as patient reception, blood sample taking, or blood quality control. The resources, represented by the *Resource* model element can be specialised into different elements: concepts of *Device*, *Software and data storage*, *Equipment*, and *Facility*. Those elements represent the typical IT resources such as a laptop, a router, etc. We completed this initial reference model by specifying the potential dependency links between OES at the ecosystem level. It has been first illustrated by the *Contract* concept between stakeholders, but we plan to define additional details here.

From the regulatory reporting point of view, each OES, in addition to its current risk report, is asked to explicit the actual relations they have with other OES. They declare partnerships and service dependencies, in alignment with the sectoral reference model. The ecosystem model is then built based on every OES reports. It encompasses the individual risk models of each OES, as well as a reconciled view highlighting the dependencies between every OES [7]. We summarise the stages

necessary to build the ecosystem model in Figure 5. The ecosystem model is then used as the input for the risk propagation step. It is worth noting that submitted data quality (i.e., about partnerships and service dependencies) is a concern and how to automate data reconciliation or at least reduce time needed for it is still an open issue.

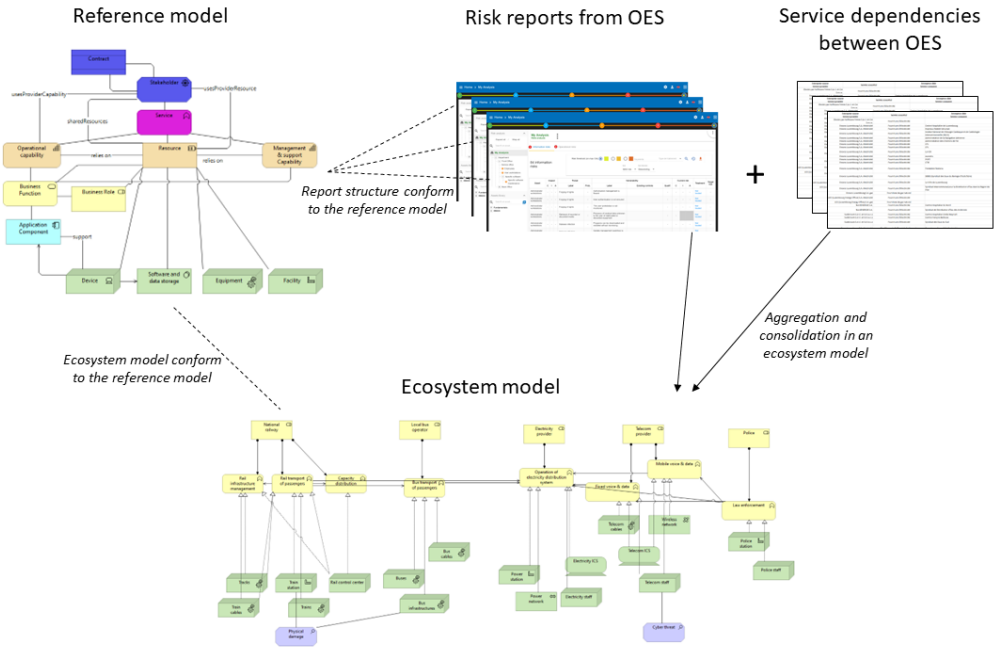

Figure 5. Ecosystem model construction based on individual reports

Risk propagation and systemic risk analysis

Before suggesting a risk propagation approach, it is necessary to have in mind the definition of a security risk and what the components of a security risk are. According to the state of the art, a security risk can be defined as '*the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization*' [8]. A risk is therefore often defined as the composition of a threat exploiting one or more vulnerabilities (also called an event) and leading to a negative impact harming some assets [9].

Consequently, the propagation of a risk from OES1 to OES2 leads to the generation of a new threat in OES2, which is the source of risk (see Figure 6). This emerging risk needs then to be identified (what

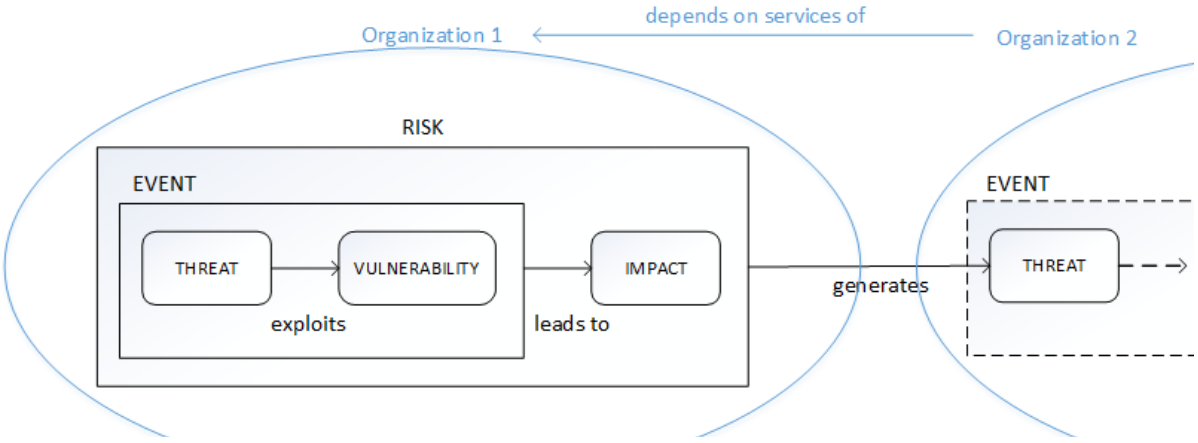

Figure 6. Propagation of a security risk

are the associated vulnerabilities and impacts) and analysed (what is the likelihood of the event and the magnitude of the impact). As an example, OES1 identified the risk of cut of a buried energy transmission cable (threat), because this cable is in an area currently under work (vulnerability), leading thus to potential stop of power supply (impact). If OES2 relies on the energy transmission cables of OES1 to provide its service (e.g., a healthcare provider), the previous risk generates the threat of 'loss of power supply' for OES2. Indeed, at the level of OES2, at the opposite of OES1, the root cause of the risk (e.g., human error, accident, theft of equipment, etc.) is out of its control (its management is under the responsibility of OES1) and probably unknown. At its level, the threat to be managed by OES2 is thus a 'loss of power supply', leading to a risk that can be mitigated through redundancy, power generator, etc.

The challenge to be addressed is to (semi-) automate the generation of the resulting threat, based on the characteristics of the risk initiator and the service it concerns. Key characteristics of the provided services are to be identified and considered. It is also crucial to know the security criteria harmed by the cascaded risk. By security criteria harmed, we mean which criteria among confidentiality, integrity and/or availability are harmed by the studied risk. For example, a risk initiated by a threat of 'fire' will potentially harm both the integrity and availability of the supported service, but not the confidentiality. At the opposite, a 'power supply failure' will only harm availability and 'corruption of data' will only harm the integrity criteria. We can then derive some basic rules such as a risk from OES1 harming integrity of transmitted data will generate the threat 'transmission and communication errors' to OES2, or a risk from OES1 harming availability of power supply will generate the threat 'loss of power supply' to TSP2. The fact that the original risk has a deliberate or an accidental cause has also been identified as a key element to well characterise the generated threat. Indeed, according to the risk taxonomy available (in these examples, we assume that the threats suggested in ISO/IEC 27005:2022 [10] are used as the reference to identify and classify the threats), a risk with an accidental cause will still lead to a 'transmission and communication error' but a risk with a deliberate cause will lead to a 'corruption of data'. These characteristics of threats are extracted from and documented in standards [10] and will be reused in our approach.

The risk analysis part of step 2 is not detailed here since it is still work in progress.

Conclusion

Due to the criticality of the information exchanged and a market more and more based on complex and integrated ecosystems, additional supervision is needed and operated by national, European, or even international authorities. These regulatory initiatives progressively allow improving the maturity of each actor and collecting data on risks. However, due to the complexity and the heterogeneity of the market, the data analysis performed by the regulators, as well as the systemic risk management regarding a complete ecosystem remains challenging.

To improve the situation, we are in the process of designing innovative tools to specifically address supply chain security. To do so, we developed an approach composed of two layers. The first one is about ecosystem modelling and systemic indicators. It focuses on actors and services at stake and their interdependencies. It is basically a graph-based framework dedicated to security and risk assessment of complex ecosystems (e.g., NIS essential services providers at a country level). The second one is about risk cascading and ecosystem risk management. It is a systemic risk management approach allowing risk cascading between dependent organisations and large-scale incident simulation. Both are currently in development in research projects in progress, with an operationalisation expected in 1-3 years.

Cybersecurity of Operational Technology

Usually when talking about cybersecurity, one thinks of the task of rendering IT and information systems secure against internal and external threats. However, nowadays, the cybersecurity of Operational Technology (OT) is becoming increasingly crucial. Especially, if one considers the growing impact of digitalisation in general and automatization of processes that underpin the fundamental structures of our societies. With our ever-growing dependency on OT, there is hence a constant need to it cybersecure OT.

OT is commonly known as the technology overall used in the industry to control and monitor physical devices and processes. This may i.e., include industrial control systems, programmable logic controllers or supervisory control and data acquisition systems. Moreover, OT is widely used in sectors that are considered “essential” for the basic functioning of our societies. For example, whether in form of electricity or in gas, OT is essential to ensure the monitoring and controlling of the generation, transmission, and distribution of energy. In the healthcare sector, OT provides monitoring and controlling of medical equipment and devices. The use of OT has become increasingly important in recent years as organisations aim to increase efficiency, improve safety, and better manage their operations.

Increasingly, OT makes more and more use of interconnected devices and networks. Due to the critical nature of such components in a variety of industries and of the interconnectivity of the devices, OT constitutes an easy target yet attractive target of cyberattacks.

In the following section, we will discuss the biggest challenges that OT systems face with respect to cybersecurity, and we will describe some best practices to help securing OT.

Challenges of OT in relation to cybersecurity

Legacy systems

At their core, OT systems are designed to control and monitor physical processes. They were not primarily built with cybersecurity in mind. As a result, legacy OT systems can be vulnerable to cyberattacks. These security gaps may cause operational disruptions, safety incidents, as well as economic impacts.

Legacy system represent hardware and software that are often outdated. They were conceptualized and installed decades ago when the fundamental need to be connected to the Internet was not yet obvious. The hardware as well as the software are usually not evident to replace or update due to the technical specificities of the domain of application. This pitfall makes it exceptionally difficult to install patches or improve the protection against new threats or attack vectors.

Increased complexity of interconnected devices

The interconnection of OT systems refers to the fact that these systems are interconnected with other systems and devices within an organisation's network. The interconnectivity is designed to allow the efficient exchange of data and information between different devices and systems, enabling them to collaborate to achieve a common goal.

However, this same interconnectivity also makes OT systems vulnerable to cyberattacks. In the case of an attacker successfully gaining access to one device within the network, he/she can spread their attack to other connected devices, potentially causing a wider network breach. This can lead to disruption of critical operations, loss of sensitive data, and potentially even physical damage to equipment.

Limited resources and different threat landscape

OT are crucial assets for providing essential services like energy, drinking water or healthcare. An attack on OT can have a critical impact on public safety, public security, and health of society. Nevertheless, the cybersecurity aspects of OT are often neglected by decision makers as awareness is missing and thus the necessary resources to improve the security of OT.

Cybersecurity cannot be treated the same way for OT as for IT, as it is a different technology as well as the usage. In the same way, the existing or emerging threats are not the same. Also, the attackers' motivation shifts from wanting to extort data to ask for a ransom or threatening to sell the data afterwards may also have a disruptive effect on the operations of the essential services. Consequently, the victim also has to face reputation issues amongst trying to mitigate the technical and functional issues.

Some guidelines and best practices

Here are some guidelines and best practices that organisations should follow to improve their cybersecurity in OT systems:

Regular risk assessments & incident response plans

Regularly assessing the risks associated with OT systems can help identify vulnerabilities and prevent potential security breaches and attacks. Organisations should also assess the impact of incidents and implement preventive measures to mitigate these risks.

Having procedures in place for different kinds of incident scenarios and the related communication to the concerned personal is of utmost importance. This allows to define procedures on how to act and react to an incident.

Segment networks

Segmenting the OT network from the IT network can reduce the risk of an incident affecting both networks. It is considered a best practice to keep the network of OT separate to the IT network of the company. This already avoids that OT can be reached through the IT applications as email or web applications that can easily be reached from the outside.

Procedures for access control and backup/recovery plans

Access to OT systems should be restricted to authorized personnel only. This can be achieved by using strong authentication mechanisms, such as multi-factor authentication, and by implementing role-based access control. Therefore, it is essential to have clear procedures in place for role assignments and access rights.

Regularly backing up critical data and having a comprehensive disaster recovery plan and business continuity plan in place can help organisations quickly recover from incidents and other disruptive events.

Awareness raising

Employee awareness and training are critical in preventing security incidents. Organisations should educate their employees about the importance of cybersecurity and provide regular training on best practices for securing OT systems as well as for IT systems.

These few guidelines provide a good starting point for improving the cybersecurity of OT systems. However, as the threat landscape evolves, it is important to regularly review and update security measures to ensure that they are effective in preventing and mitigating security incidents. As this is just a very brief introduction to the guidelines it is advised to go into more detail. For instance,

checking the ENISA guidelines on security measures [11] could be an option. These guidelines were issued for the specificities of the telecom sector. However, the security objectives defined in it, are relevant and beneficial to all kinds of sectors for a higher level of cybersecurity.

In conclusion, securing OT systems is essential to protecting essential services and maintaining the reliability of industrial processes. While there are challenges to overcome, implementing best practices can help reduce the risk of cyberattacks and ensure the security of these systems.

Risk management: first cycle feedback and improvement opportunities

One security requirement of the NIS Directive [1] states that OES "*should take appropriate and proportionate technical and organisational measures to manage the risks posed to their information systems*". Those measures will of course evolve through time and adapt to the threat landscape. An effective way to comply with this requirement is by conducting a yearly risk assessment. However, like any compliance requirement, we need to ensure that it has a positive impact on the information security of the OES. Otherwise, the analysis could be carried out only for compliance purposes.

Limitations

When a regulatory authority asks for a risk assessment to an operator, several limitations may affect the accuracy and completeness of the assessment. Hence, the added value of this request may be absent.

Limitations that we have seen during the set-up of the risk assessment process include:

- **Limited data availability:** The operator may never have collected the data to accurately assess the risks (e.g., threat likelihood, the impact of scenarios, etc…).
- **Lack of expertise:** The operator may not have the expertise to fully evaluate the risks in all risk areas.
- **Time constraints:** The operator may be under time constraints to complete the assessment which could lead to incomplete or inaccurate results.
- **Bias:** The operator may have a vested interest in the outcome of the assessment, which could lead to bias in the results.
- **Assessment difficulty:** It can be difficult to assess the current threat likelihood or to accurately assess a scenario's impact. The larger the scope, the more types of threats and vulnerabilities need to be considered, which can lead to too much complexity and would prevent the assessment from being relevant and objective.
- **Static assessment:** The purpose of a risk assessment is to find out what current risks the organisation faces and to identify the current state of the company's measures against it. Doing the risks assessment once per year can lead to a static update that is not adapted to the current geopolitical, economic, and technological context.

All those limitations can lead to a low accuracy risk assessment that will be made once a year purely for legal requirements. The impact on the organisation's security would be low.

Expectations

To enhance the risk assessment process, we should focus on the outcome of this analysis. From the perspective of the regulatory authority, the goal is to have a complete view of the risk landscape of the sector. The knowledge of the most impactful risks, the most likely threats and the current operator measures is a top priority to maintain the continuity of OES. For the operator, the assessment is a good tool to focus the security strategic plan on the threats they are really facing.

How to achieve expectations?

First, the risk assessment process should be clear and common to all parties and the plan should include every step that is needed to avoid or reduce those limitations.

The first identified limitations are related to a lack of resources and expertise to evaluate the risk of the company. The regulatory authority has a strategic position to collect information and to

coordinate the support of other administrations: CERT, cybersecurity authorities, national crisis centre and other authorities. Altogether, they might have a better view of the threat landscape and complementary information to prioritize the risks. It is also important to set up a way to share data between operators. This collaboration can lead to the establishment of a shared knowledge base that will reduce each operator's time to analyse threats. The scope definition will also be much easier with this approach.

To avoid static assessments, it is necessary to include the risk assessment in a study of the sector's risk context. This needs to be done at least once a year before every risk assessment cycle. Eventually, it could be updated multiple times a year. Of course, this step is meant to be made collaboratively between operators and the regulatory authority. By implementing this discussion, the sector can also define the scope of the risk assessment. A well-defined common scope will ensure the same level of granularity between multiple risk assessments and will lead to relevant analysis for the sector. The ecosystemic analysis approach explained in the first section of this document (p.6) could also be a great way to enhance this process as it gives the stakeholders a better risks view of the sector.

Within this context, it is important to dynamically share data with the OES. Depending on the threat landscape, the regulatory authority can require mandatory threats to assess or update the threats and vulnerabilities libraries. It is relevant to suggest points of attention to the sector. Using data from other activities between operators and regulatory authorities can also make the process more dynamic: incident management and reporting, inspections/audit, and information sharing.

At the end of a yearly risk assessment, the regulatory authority should pay attention to the fact that the analysis of the assessment results is essential for the next round. One impact of the assessment request for an operator is the potential feedback and insights from the neutral perspective of the regulator.

In conclusion, the risk assessment should be a cycle of dynamic information sharing and analysis followed by feedback from the regulatory authority. This process must be clear to all parties involved. Multiple regulatory activities can provide information to the risk assessment process: inspections, incident reporting and communication with other sectors and authorities. In the end, it is important to review the whole process and the impact of the risk assessment. The right scope and methodology are crucial to make an impactful risk assessment. It is thus relevant to adapt it at the end of the cycle.

Lessons learnt from Computer Security Incident Response Teams (CSIRTs)

In this section, best practices are proposed from the perspective of the Computer Incident Response Center Luxembourg (CIRCL), the CSIRT for the private sector, communes, and non-governmental entities in Luxembourg. Referring to Art. 9 (1) of the NIS Directive [1], a Member State designates one or more CSIRTs to comply with the requirements set out in point (1) of Annex I, covering at least the sectors referred to in Annex II and the services referred to in Annex III, and responsible for risk and incident handling in accordance with a well-defined process. For the local NIS Directive implementation in Luxembourg, two CSIRTs were referenced: GOVCert and CIRCL, with GovCERT focusing on governmental entities and CIRCL on the private ones.

Evidence-driven reporting from an incident response perspective

A common point of the various regulatory authorities reporting duties is that they generally require to define the related impact. These questions are not always easy to answer as they imply a detailed analysis. To perform these analyses, related data must be available and that implies the various compliance activities are achieved in advance. Common compliance activities are the elaboration of GDPR processing activities. The added value of GDPR is that not all processing activities need to be previously approved by the data protection authority. Hence, data processing activities can be adapted to the reporting obligations by other regulatory authorities.
This section has a perspective from an incident response perspective where entities voluntarily contact a CSIRT for remediation and analysis of incidents. A commonly observed pattern is that the evidence acquisition chain is often not ready to have the necessary data available to answer the question of the regulatory authority. An update of the evidence acquisition involves multiple teams as GDPR processing activities are subject to be updated.

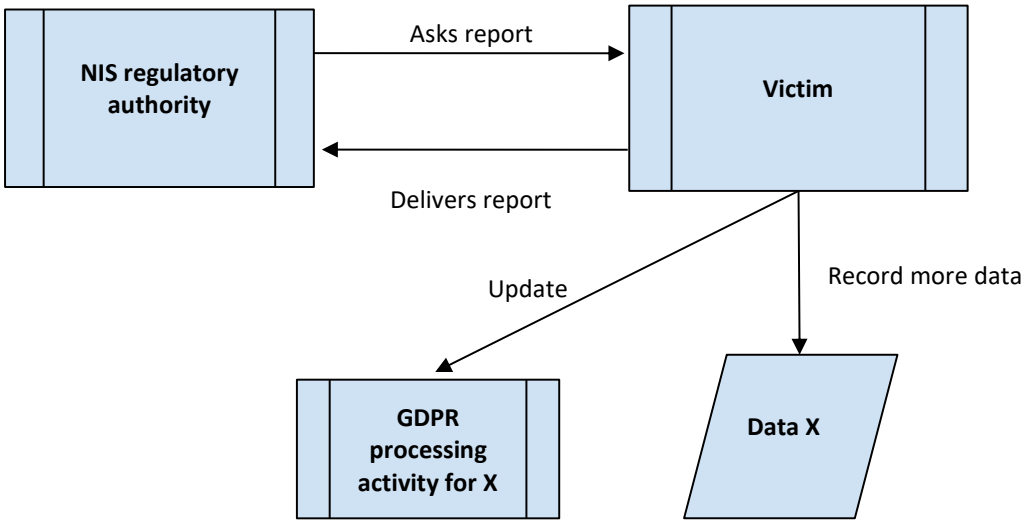

Figure 7: Evidence acquisition chain

Often, entities are regulated by many regulatory authorities. In case the entity is represented in multiple countries, the authorities are multiplied. As an illustrative example, in Luxembourg, when personal data is involved, for instance in a data leak, then the CNPD[2], as the data protection authority,

[2] Commission Nationale pour la Protection des Données

must be notified. If the same entity is OES, the ILR[3] or CSSF[4] (for Banking and financial market infrastructures), as the sectoral NCA, must be notified. Each regulatory authority has its own questions triggering the handling of dedicated evidence. Some of them have temporal constraints. For instance, data leaks must be reported in less than 72 hours to the competent authority.

The question can be formulated as follow:

Do I have the necessary data based on evidence to answer the question of each regulatory authority?

Although this question sounds simple, it is sometimes difficult in practice. This is due to the gap between the compliance team and the operational team capable of extracting the data. However, there is another complexity that is observed: the correlation of data. The compliance team is collecting the data by querying the operational team for various pieces of evidence, but if multiple systems are involved to answer the question, a correlation of pieces of evidence must be made. Then, this correlation should be tested in advance to ensure that the chain can be followed.

An example is an exploited service behind a proxy, as shown in Figure 8. In this example, the attacker performs an injection (for instance a SQL injection). The proxy records the IP address of the attacker. The server logs the IP of the web proxy and the URL. An analyst detects in the URL the injection attack but sees only the IP address of the proxy. Hence, a correlation must be made between the log records of the web proxy and the webserver.

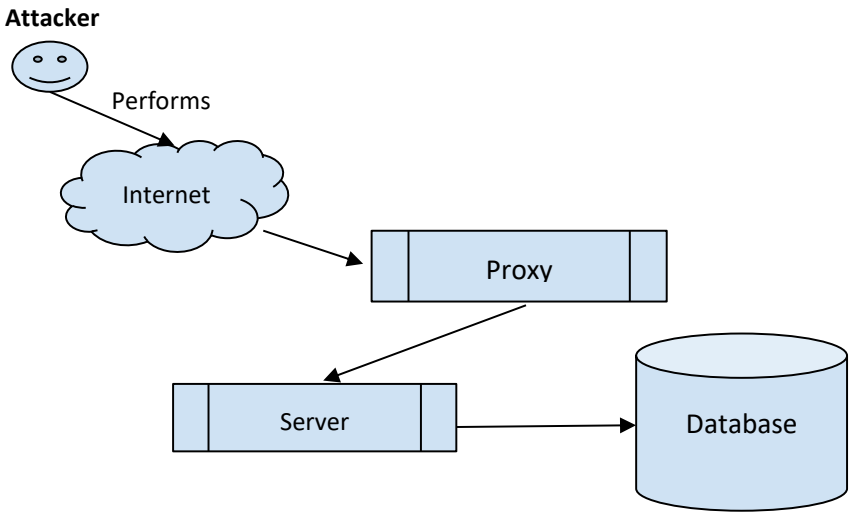

Figure 8: Example of an exploited service behind a proxy

Also, what is frequently observed is a lack of evaluation of the evidence, rendering them useless to answer the questions asked by the regulatory authorities. In some cases, the formal processes were defined to acquire the evidence, however they were not properly evaluated. Typical defective pieces of evidence are listed below:

- **The logs were extracted from the wrong time window.** The attack happened at time T-1 and the logs were extracted from time T. This either happens, if the operator extracts the wrong logs or if the old ones were overwritten in case a ring buffer is used for logging.

[3] Institut Luxembourgeois de Régulation
[4] Commission de Surveillance du Secteur Financier

- **Relative or partial timestamps.** Timestamps are often integers representing relative time, but the reference time was not recorded. Timestamps are often found in incomplete date formats, for instance a component of the date is missing such as the year, month, day.
- **Pre-interpreted logs.** In the case of a crash investigation, the operators send the logs of the crash of the wrong process.
- **The logs are in a proprietary format where a dedicated software and a license is needed to read them.** In case the operators have these licenses, they can use them but if the analysts don't have them, they cannot use them.
- **The hardware and operating specifications are not available.** This is important for the analysis of memory or crash dumps. The architecture and the operating system must be known to properly analyse the crash dump.
- **File components are missing to analyse the files.** This happens in case of analysis of crash dumps when the binary is missing.

Out-of-band communication

With the observed abused and compromised email servers such as Microsoft Exchange[5] servers or the Zimbra[6] email servers, not only data privacy was impacted with the leak and abuse of mails but also disruption of the communication channel between the victim and the incident response teams or regulatory authorities. As attackers control the email infrastructure, they could block emails to incident response teams or regulatory authorities. In a worse case, attackers could even tamper with the communications, by injecting for instance malicious payload to the reported reports send to the competent authorities. Hence, sending reports in plain text, without any cryptographic protection is a risky operation. Some regulatory authorities [12] use PGP keys that can be used by the victims to encrypt their reports before sending. However, from the regulatory authority's perspective, it is not certain that the report was sent from the victim or by the attacker.

The tricky part is the assessment of the infrastructure or the following question:

Is the infrastructure trustworthy enough to communicate with the regulatory authorities?

In case of a taken over infrastructure, attackers have the following opportunities as illustrative example:

- Block the communication with the regulatory authorities.
- Interfere with the communication with the regulatory authorities. Typical interference patterns observed are the addition of malicious links or payloads in the documents sent to recipients by the victim. Hence, the regulatory authorities could also be impacted.
- Impersonate the victim at the regulatory authorities. In this case, the attacker sends reports himself to the regulatory authorities instead of the victim.

Hence, CIRCL recommends its constituents to be prepared for out-of-band communication, including its additional GDPR processing activities. For emails a third-party email service could be used, records with accessible phone numbers to reach the various stakeholders in case of complete outage of the IT

[5] https://www.microsoft.com/en/microsoft-365/exchange/email
[6] https://www.zimbra.com/

infrastructure. A paper version of phone lists is an effective protection against targeted ransomware attacks disrupting backups, backup sites and operational IT.

In case, suddenly people had to switch to voice communication, communications errors were often observed, especially with the transmission of words that are not in a dictionary such as IP addresses, codes, cryptographic digests etc. In that case, CIRCL advises to use phonetic alphabets, codes, and signals such as the one from NATO [13].

A challenge is, within a time constraint regulatory authorities, to assess which parts of the infrastructure were impacted from a practical point of view. Sometimes, it gets visible in monitoring systems, sometimes by descriptions of symptoms by the users, or external reports. For instance, if customers cannot access the content management systems anymore, employees cannot write emails or make phone calls. External reports must be examined carefully. Frequently, organizations get notified that their infrastructure is compromised, but an investigation shows that the attackers used a fake infrastructure impersonating the victim. In this case, the infrastructure of the victim can still be used.

Cerebrate

In the CSIRT community, in the MeliCERTes consortium under the DG-CNECT procurement contract SMART 2018/1024 [14], CIRCL developed the Cerebrate tool [15], that is used in large decentralized MISP [16] topologies to ensure the veracity of the MISP instances relying on cryptographic verification mechanisms. This tool helps to manage cryptographic key material in a sharing community. However, it needs some prior setup and cryptographic material exchange and verification mechanisms. Once the cryptographic material is encoded in a Cerebrate, the other Cerebrate instances can query it and even the interconnected MISP instances can query it.

List of abbreviations

Abbreviation	Translation
CIRCL	Computer Incident Response Center Luxembourg
CNPD	Commission Nationale pour la Protection des Données
CSIRT	Computer Security Incident Response Team
CSSF	Commission de Surveillance du Secteur Financier
DSP	Digital Service Provider
EECC	European Electronic Communications Code
GDPR	General Data Protection Regulation
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
NCA	National Competent Authority
NISDUC	NIS Directive User Community
OES	Operator of Essential Services
OT	Operational Technology
PGP	Pretty Good Privacy
SPOC	Single Point of Contact
SQL	Structured Query Language
URL	Uniform Resource Locator

Terms and definitions

Cloud computing service	A digital service that enables access to a scalable and elastic pool of shareable computing resources [1].
Digital Service	Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services [1]. For the scope of the NIS Directive, only three types of services (as defined in Annex III of the Directive) are considered: • Cloud computing service. • Online marketplace. • Online search engines.
Digital Service Provider	An entity that provides digital service(s).
National Competent Authority	An authority designated by each Member State in charge of monitoring the application of the NIS Directive at national level [1].
Network and information system	(a) an electronic communications network within the meaning of point (a) of Article 2 of Directive 2002/21/EC, (b) any device or group of interconnected or related devices, one or more of which, pursuant to a program, (c) perform automatic processing of digital data; or digital data stored, processed, retrieved, or transmitted by elements covered under points (a) and (b) for the purposes of their operation, use, protection, and maintenance [1].
NIS Directive	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms [17].
Operator of Essential Services	A public or private entity of a type referred to in Annex II of NIS Directive, which meets the criteria laid down in Article 5(2) of the NIS Directive [1].
Risk	Any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems [1].
Security of network and information systems	The ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems [1].

Security risk	The potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization [8].
Single Point of Contact	An entity designated by each Member State in charge of exercising a liaison function to ensure cross-border cooperation of Member State authorities and with the relevant authorities in other Member States and with the Cooperation Group and the CSIRTs network [1].
SQL injection	A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands [18].

Bibliography

[1] Official Journal of the European Union, *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*. 2016. [Online]. Available: http://data.europa.eu/eli/dir/2016/1148/oj

[2] Official Journal of the European Union, *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj

[3] Official Journal of the European Union, *Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code*. 2018. [Online]. Available: http://data.europa.eu/eli/dir/2018/1972/oj

[4] N. Mayer and J.-S. Sottet, '*Systemic Security Risks in the Telecommunications Sector: An Approach for Security and Integrity of Networks and Services*', in *5th International Conference on Complexity, Future Information Systems and Risk*, pp. 72–79.

[5] M. M. Lankhorst, H. A. Proper, and H. Jonkers, '*The Architecture of the ArchiMate Language*', in *Enterprise, Business-Process and Information Systems Modeling*, 2009, pp. 367–380.

[6] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa, '*An integrated conceptual model for information system security risk management supported by enterprise architecture management*', *Softw Syst Model*, pp. 1–28, 2019, doi: 10.1007/s10270-018-0661-x.

[7] J. Sottet, E. Grandry, and M. Bjekovic, '*Managing Regulatory System with Megamodelling*', in *2018 IEEE 20th Conference on Business Informatics (CBI)*, Jul. 2018, vol. 02, pp. 1–10. doi: 10.1109/CBI.2018.10041.

[8] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. Geneva: International Organization for Standardization, 2018.

[9] É. Dubois, P. Heymans, N. Mayer, and R. Matulevičius, '*A Systematic Approach to Define the Domain of Information System Security Risk Management*', in *Intentional Perspectives on Information Systems Engineering*, S. Nurcan, C. Salinesi, C. Souveyet, and J. Ralyté, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 289–306.

[10] ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Geneva: International Organization for Standardization, 2022.

[11] European Union Agency for Cybersecurity (ENISA), *Guideline on Security Measures under the EECC*, July 07, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc

[12] Data breach notification PGP key of CNPD. https://cnpd.public.lu/dam-assets/fr/declarer/databreach-pub-key.asc

[13] NATO phonetic alphabet, codes and signals, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_01/20180111_nato-alphabet-sign-signal.pdf, 2018.

[14] Ted-eTendering, Call for tenders' details, SMART 2018/1024, Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs - MeliCERTes Facility, European Union, https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4340

[15] Cerebrate Project, https://github.com/cerebrate-project
[16] MISP Threat Sharing, https://www.misp-project.org/
[17] U.S. Department of Commerce, National Institute of Standards and Technology (NIST), *Risk Management Framework for Information Systems and Organizations -- A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37, Revision 2. December 2018. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-37r2
[18] OWASP Foundation, SQL Injection, https://owasp.org/www-community/attacks/SQL_Injection