An Information Flow Model for the Support of NIS Mandated Reporting

Gerald Quirchmayr[1],Veronika Kupfersberger[1],
Gregor Langner[1],Thomas Schaberreiter[1]

[1]University of Vienna, Faculty of Computer Science, Multimedia Information Systems Research Group Whringer Strasse 28, A-1090 Vienna, Austria

[Gerald.Quirchmayr, Veronika.Kupfersberger,
Gregor.Langner, Thomas.Schaberreiter]@univie.ac.at

Abstract: After briefly motivating the research and listing the major challenges resulting from the NIS Directive, this contribution presents an information flow model which is, amongst other goals, aimed at supporting reporting obligations mandated by the NIS Directive. The model and its components are then described, followed by an example of the models information sharing and exchange component as it is currently used in the CS-AWARE project. The paper finishes with an outlook and conclusions.

1 Introduction

The European Union has introduced a series of new legislation [1] [2], aimed at countering the growing number and sophistication of threats against security and privacy. With the criminal and political landscapes changing for the worse [3], this consolidated European legislative response comes at the right moment, trying to balance the necessities of protecting ICT infrastructures with privacy requirements. Especially against the background of Industry 4.0 becoming a major cornerstone of the European economy [4], this new legislation can be expected to have a major societal impact. With critical infrastructures and significant digital services being the focus of the NIS Directive, the protection of vital societal services now receives the much needed legal attention [10].

2 Major new obligations introduced by the NIS Directive and arising challenges

The major obligations introduced by the NIS Directive are concerned with the protection of vital infrastructures and reporting duties in case of major incidents.

The primary goal of the legislation is to enhance the resilience of critical infrastructures and to establish an early warning mechanism that allows a coordinated response. As a reliable infrastructure and a dependable network between trusted partners are crucial for the successful implementation of truly European information sharing, protection and coordinated response mechanisms, a network of trusted nodes is needed. In this situation the obvious choice was made - giving national and sector CSIRTs a central role in coordinating these efforts. These elements of the Directive were translated into national legislation in European Union Member States over the past years and are now being applied. Especially the resulting mandatory reporting duty for significant cyber incidents is expected to be a major game changer regarding the situational awareness in Member States and ultimately across the whole European Union. One of the resulting major challenges for affected organizations now is to put in place a situational awareness tool that allows them to identify, detect and report indicators of a major attack and to correlate events across the organization, which is even more difficult in case of a distributed ICT environment.

3 An information flow model for the support of NIS mandated reporting

Given the challenges described in the previous chapter, the need for a support tool is obvious. In order to build a sustainable approach, an information flow model [5] was developed to feed a situational awareness framework, including the reporting functionality mandated by the NIS Directive. In order to be effective, this information flow model is aimed at helping to identify attacks, supporting the application of counter measures and providing enough information about an attack to allow a meaningful reporting. The architecture is described in Figure 1.

As can be seen from the illustration above, the model comprises several relatively independent components. This approach was chosen to allow a flexible execution, because not every organization needs all of the components. The functionality of these components is as follows [6]: As basis for further analysis, a System Dependency Analysis is carried out as starting point. **The System Dependency Analysis** is performed by combining the Soft Systems Methodology and the GraphingWiki, resulting in a strategic implementation process for the concerned organization. Based on the pilot analyses, guidelines for future System Dependency Analyses will be developed. The next step is focused on **Data**

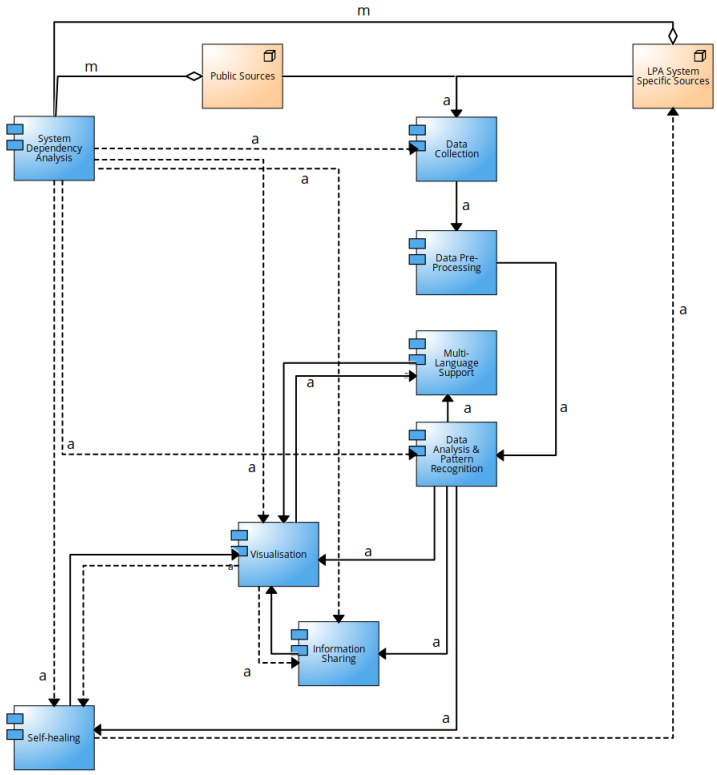

Fig. 1: The CS-AWARE Information Flow Model [5]

Collection. The Data Collection component will be responsible for developing the data collectors for system specific data as well as external sources. The Cybersecurity Information Exchange module is responsible for sharing information on detected attacks with authorities, according to the NIS regulations. **The Cybersecurity Information Exchange** will allow the user to individually authorize any transmission before it occurs. A Visualization component covers the final data manipulations required for graphically representing the collected information as well as the construction of the user interface. The Self-Healing component will receive information from the Data Analysis module and compose Security Rules based on the detected incident. These rules can then be applied to the systems by the respective IT departments. The **Data Pre-Processing** component executes pre-defined strategies, one of them being the **Natural Language Processing** for Information Extraction, which is a simplification process of textual information. Other possibilities would include the simple filtering of known irrelevant data or the transformation of data formats. Due to the European context of CS-AWARE, the final UI should include not only easily understandable visualizations but all text in either the native language of the end user or English. **Multi-Language Support** is therefore required.

As security solutions do heavily depend on an organizations policies [7], any implementation of the model will have to cover on site, cloud based and hybrid variations. That is the major reason why Docker containers were chosen as basis for the system architecture. Another advantage of this approach is a high flexibility in orchestrating execution paths that usually vary from organization to organization.

4 Application of the information flow model in local public administrations[8]

The first context in which this information flow model and the related framework were applied is the CS-AWARE project, which is aimed at providing local public administrations with a tool that creates the necessary awareness in case a cyberattack occurs. As especially larger local public administrations also run critical infrastructure services that come under the NIS Directive, such a framework and the related tool support are a highly welcome resource. The major user group to be provided with awareness raising information are system and information security administrators, because they are the ones who most need a big picture of an attack situation to be able to identify the target of an attack and the modus operandi of an attacker. As important as a forensic evidence collection is for attributing an attack to an attacker, the major goal of this information flow model is to support those who are charged with defending an attacked system. The primary use cases therefore are the detection of vulnerabilities and the identification and classification of an attack. Both goals are in line with the NIS Directive, strengthening existing defenses and improving early warning capabilities. In this context the visualization component acquires a central role, pointing the user directly to where a problem occurs. Regarding the incident reporting obligation introduced by the NIS Directive, the **Cybersecurity Information Exchange** module plays a core role. The docker container architecture used in the project is shown in Figure 2.

Table 1 gives an overview of the docker compose commands and their parameters as used in the CS-AWARE project.

In order to be open for future developments, the STIX/TAXII [9] standards are applied as basis for communication and information sharing, both internally and externally. As these two standards now also starting to be introduced in smart manufacturing infrastructures, embedding the developed information flow model in cyber physical systems becomes a viable option.

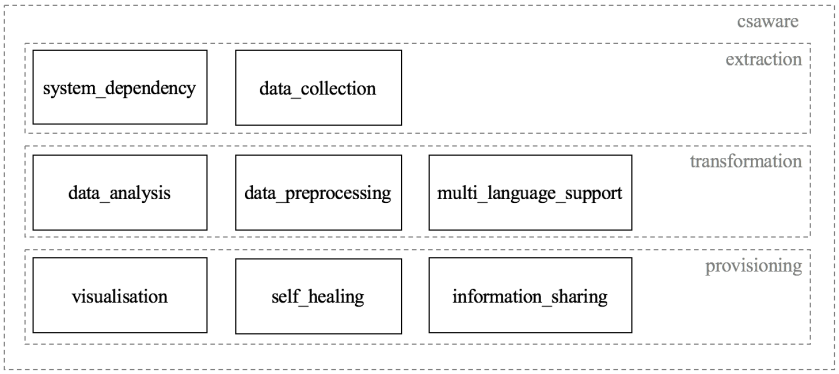

Fig. 2: CS-AWARE Docker Container Architecture [6]

Table 1: Docker Compose Commands and their Parameters used in CS-AWARE [6]

Commands	Parameters	Definition
build	context dockerfile	Any information relevant at build-time is specified here Location of built container is specified. If required, the path to an individual dockerfile for this specific container can be specified here
restart		Containers can be told to automatically restart after shutdown either on failure, always or unless-stopped
networks		Either the default network created by Docker Compose is used or individual networks can be defined
	aliases internal	Container can have aliases in each network they are allocated to In internal networks, only other containers of the same network can gain access
logging ports		Activates the automated logging function of Docker Individual ports can be defined for each container, which are opened and can be accesses by other containers or external software
image		Can either be a new name for the created container or an existing image can be loaded here

5 Outlook and Conclusion

Given the reporting obligations introduced by the NIS Directive, tool-supported models such as the one presented in this paper will become a common necessity for critical (information) infrastructure protection. Defensive measures, especially the fast identification and detection of threats, will play a decisive role in making our ICT infrastructures more resilient and will be essential for establishing an EU wide early warning and response coordination system [10]. Especially the reporting network which is bulding on national and sector CERTs is expected to become a major game changer once it is fully operaaational [11] [12]. This is another reason why the presented information flow model has a high potential beyond the public sector.

6 ACKNOWLEDGEMENTS

he authors would like to thank the EU H2020 project CS-AWARE (grant number 740723) for supporting the research presented in this paper.

References

[1] The Directive on security of network and information systems (NIS Directive) (2016b) https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). (2016a)

[3] The 2018 Internet Organised Crime Threat Assessment, Europol, 2018, available on https://www.europol.europa.eu/sites/default/files/../iocta2018.pdf

[4] Bogoviz A.V. (2019) Industry 4.0 as a New Vector of Growth and Development of Knowledge Economy. In: Popkova E., Ragulina Y., Bogoviz A. (eds) Industry 4.0: Industrial Revolution of the 21st Century. Studies in Systems, Decision and Control, vol 169. Springer, Cham, ISBN 978-3-319-94309-1, https://doi.org/10.1007/978-3-319-94310-7_8

[5] Kupfersberger, V., Schaberreiter, T., Quirchmayr, G., Security-Driven Information Flow Modelling for Component Integration in Complex Environments, *in Proceedings of the 10th International Conference on Advances in Information Technology* (2018), ISBN 978-1-4503-6568-0.

[6] Kupfersberger, V., The CS-AWARE Information Flow Model, Masters Thesis at the Univeristy of Vienna, 2018, supervised by Gerald Quirchmayr and Thomas Schaberreiter.

[7] Safa, S.N.,Von Solms, R., Furnell, S., Information security policy compliance model in organizations, in Computers & Security, Volume 56, February 2016, Pages 70-82, https://doi.org/10.1016/j.cose.2015.10.006

[8] EU H2020 project CS-AWARE (grant number 740723), https://cs-aware.eu/

[9] Cybersecurity and Infrastructure Security Agency, Information Sharing Specifications for Cybersecurity, https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

[10] European Union Cyber Security Strategy, https://ec.europa.eu/digital-single-market/en/cyber-security

[11] ENISA on CSIRTs network, https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

[12] ENISA Study on CSIRT landscape and IR capabilities in Europe

2025, V 1.0 — February 2019, https://www.enisa.europa.eu/publications/study-on-csirt-landscape-and-ir-capabilities-in-europe-2025