National Cyber Security Centre
Ministry of Justice and Security

The need for a Cyber Security Information System

Non-paper on Europe-wide incident reporting under NIS 2

The Network and Information Security 2 Directive (NIS 2) was officially published in the EU Official Journal on December 27th, 2022, meaning that the implementation phase has started. As a result, Member States will have an implementation period of 21 months to transpose the NIS 2 Directive into national legislation. That will be easier said than done, as some aspects of NIS 2 remain open or cannot be resolved by a single Member State. One such example is cross-border incident reporting by Member States. At present, there is no functioning system in which incident notifications can be exchanged between EU members apart from manually through the CSIRT network.

This non-paper argues for the creation of a structure similar to the Schengen Information System, EURODAC or EUCARIS system to enable the CSIRT community to report Europe-wide cyber incidents. It starts with the legal foundations of a cyber-Security Information System (cyber-SIS) and then focuses on the practical aspects.

Legal foundations

The foundations of the incident reporting lie in Article 23.6 of NIS 2, which states that essential and important entities shall report cyber incidents: “Where appropriate, and in particular where the significant incident concerns two or more Member States, the CSIRT, the competent authority or the single point of contact shall inform, without undue delay, the other affected Member States and ENISA of the significant incident.”

There are several reasons why the NCSC-NL believes that NIS 2 will generate a lot of ‘incident reporting traffic’ that is currently handled manually. First, the benchmarks for incident reporting will be lower and the legal constituency will be much larger. Secondly, a majority of the (new) entities work on a cross-border basis or have multiple offices or service stations in the EU. Thirdly, practically all soft- and hardware is used across borders (and not exclusively by one Member State). In addition, some sectors, like DNS service providers, are required to inform the Member State about their ‘main establishment’, creating additional complications in incident reporting traffic (Article 26.1). To solve the latter problem, the registry will be part of the solution (Article 27), but it is still unclear how this is to be set up between Member States.

How then, do we forward incident notifications and how do we know which Member State has a genuine interest in receiving the notification if we do not have a central registry? How do we answer the call to limit inefficiency and avoid entities having to report in each and every Member State where it has ‘important or essential’ operations?

The idea behind a system for the CSIRT community

The Schengen Information System (SIS) is the information sharing system for security and border control management in Europe. EURODAC is active in the field of immigration, while EUCARIS is related to vehicle registrations. Those systems share information between different stakeholders and all operate on the basis that the originating Member State is, and remains, the owner of its own data.

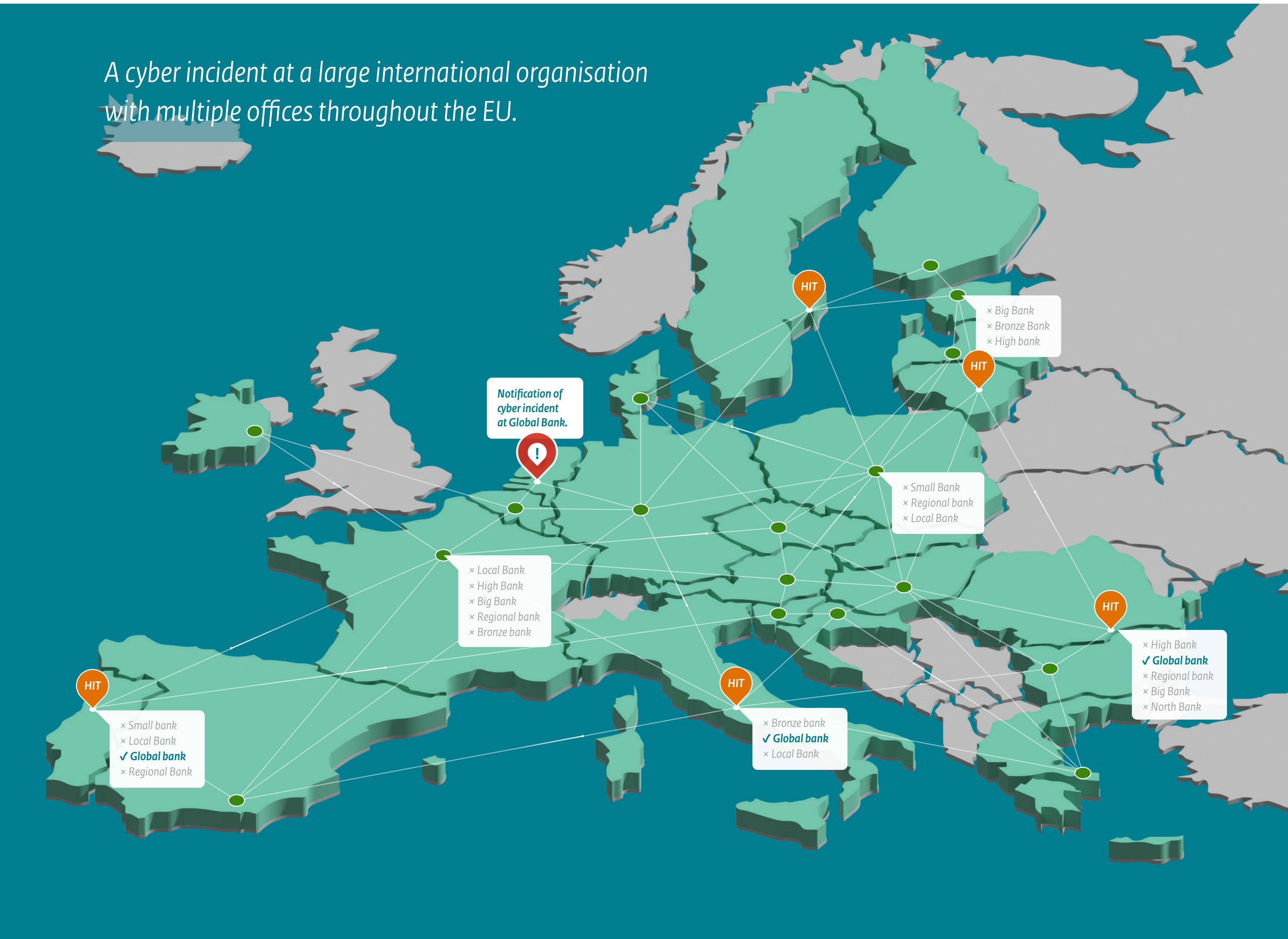
The systems operate by means of alerts, meaning that Member States identify people or objects of interest in their national database. Alerts are entered in the systems on the basis of identification data. This can be, for example, missing persons, refusal of entry or stay and persons sought for a judicial or criminal procedure. The country that enters the alert and related data in the system is the 'data owner'. This means that only this country is allowed or able to update and delete the alert. The national authority that carries out the check on the person or object will notice a 'hit' and is informed automatically about the reason why this person or object is being sought and what is required of the Member State (or alert or data owner). How will this model help CSIRTs with incident notification handling?

For the NIS 2 Cyber Security Information System (Cyber-SIS)

This paper has argued that incident notification traffic will increase substantially. Forwarding notifications manually and in a tailor-made fashion is unrealistic for national authorities. In addition, using the existing CSIRT network for this purpose might overload the network and compete with the other tasks it is designed to perform.

The NCSC-NL therefore calls upon the Commission, ENISA, and other stakeholders to facilitate a safe networking-based system for the CSIRT-SPOC community. The working title could be cyber-Security Information System (or cyber-SIS). The idea behind cyber-SIS is that every Member State has and maintains its own list of important and essential entities (in line with Article 3.3). That list is stored on national servers. When one country receives an incident notification with a predetermined set of parameters, that incident notification can be forwarded to cyber-SIS and can then be sent automatically to all EU Member States and ENISA. Cyber-SIS will check whether it has a corresponding hit on an entity that the other Member State(s) has/have also defined as essential or important. If so, the receiving Member State(s) and the originating Member State will automatically receive the (incident) notification. If the Member State has not defined the entity as essential or important, it will not receive the notification. The originating Member State will receive a notification stating which Member States are interested in the notification. In this regard, cyber-SIS works on a need-to-know basis (in line with the NIS 2 legal requirements). Cyber-SIS could be enriched in future by also including the requirements under the Cyber Resilience Act, vulnerability notifications or other legislation (i.e. DORA).

Below is a schematic diagram showing how cyber-SIS should work:



A cyber incident at a large international organisation with multiple offices throughout the EU.