Interview regarding the Annual major cyber incidents 2012 report according to Art 13a

With Christoffer Karsberg, expert at ENISA

What is new in this report and why is it important for Europe?

ENISA Expert,Christoffer Karsberg is the project manager of the 2012 Incidents Report.

-That is a big question, to start with, but OK, it is good to get the broader picture. Earlier, we knew that there are cyber incidents occurring, but we did not know the magnitude and the features of them. By receiving incident reports at the European level, we can aggregate the results, and provide a picture of the overall pattern of the incidents. This is very useful when providers, the National Regulatory Authorities-the "NRA"s, and politicians discuss how to take measures, what measures to take, and what services they should focus on.

-Moreover, this becomes a very useful tool for discussing priorities. And also for incidents per se; what were the causes of the incidents? How were these incidents managed? This is not something we detail in the report, but the report triggers these discussions. As such it is very useful for providers and user communities, to discuss their experiences and how to address them.

-And also since we are doing this report only for the second time around, it is too early to draw far reaching conclusions of them. But after a few years, we will hopefully see how incidents behave over time, and we can identify a pattern more clearly. We can then see how they increase and decrease, apart from what are normal fluctuations.

-This report is also important information for the security priorities. With this report, we can make recommendations and soon, in a few years, make a better "diagnosis" of the symptoms, and can also eventually look at the suitable medicine and treatment for Europe, to be discussed and undertaken by the Member States authorities.

What is Article 13a really about?

-It is about two things:

Firstly, an obligation for providers to take communication measures to guarantee the functioning, security and integrity of their networks, which is defined in the directive

regarding electronic communications, such as fixed/mobile telephony and fixed/mobile Internet, and their accessibility.

-Secondly, an obligation for providers to report to the National Regulatory Authorities (the NRAs of incidents and breaches that have occurred in these services. I also want to say that services are defined together with the NRA, but this does not exclude them to make providers report also about other incidents.

-For example some NRA see SMS as important, and have reporting schemes for this. Others have broadcasting in their focus, so it is up to the NRA to define what they see as any key and relevant additional electronic communication services to report about.

Then the NRA has to report to ENISA and the European Commission on an annual basis. In addition to this, if there is an incident that has or may have cross border impact, the NRA informs other relevant NRAs and ENISA about the incident.

-One important part of this is to share the analysis, and to improve by sharing results across Europe. Obviously, the EU Commission can use this to build statistics and priorities for the political discussion, and drafting recommendations and future regulation. So it is important for the European Commission to have this knowledge database coming, over the years, where ENISA provides the analysis and issues this report.

Was there anything in the report which surprised you?

-I do not want to make too many comparisons with 2011, as the number of reports was a bit limited, and we need to be cautious, as we only have two years of empirical studies.

-So it is too early to say much about that. It could be normal, statistical coincidences or temporary tendencies. For instance, last year we had many storms that showed one type of structure of the incidents, which we do not see this year. But eventually, gradually, this is what this annual report is about; it will function as a thermometer of the state of major cyber security incidents in the EU.
-But still, given this disclaimer, what surprised me ,was how many incidents were related to system failures. Around 75% were systems failures. And this is something that we took notice of.

For most incident reports, as well as for the four services, the root cause was "System failures" (75 %).

-Because what does this mean? Clearly, electronic communications are becoming more dependent on hardware and software availability. It is not so much cable cuts, and traditional types of incidents. They still have a high percentage of incidents, but system failures really need attention. We need to work on robustness of hardware and software.

This is in indication of where telecom meets IT, and where IT equipment becomes more critical for the availability of these services.

-This is also a milestone in collaboration for Europe; the EU MS cooperating on sharing these results; we did not do that before. Therefore, this is a new step, in creating a closer and successful cooperation within the EU on this; by sharing information across borders in the cyber security sector, in between administrations. This way, we all learn, and take better actions to prevent them from happening. So, we are very pleased with how well the Member States are working with us on this.

What more is new here is that we have established and refined the technical parameters for when reporting should be done, with common thresholds to define a major cyber incident, across Europe. We will also continue to do so, to take this one level higher, with the NRAs.

What kind of incidents are we talking of, what does the structure look like?

-We can categorise them into route cause categories, and separate them in big chunks:

- Systems failures
- Natural phenomena
- Human errors
- Malicious actions
- Third party failures, which are outside the control of the provider who has the incident.

Incidents caused by overload followed by power failures respectively had most impact in terms of number of users affected times duration.

When we dig deeper into these caterings, we can find overload incidents, causing congestion and interruption of services, software bugs, and also natural phenomena, like heavy snowfall.

Also, in some instances there were cyberattacks. That is, deliberate actions aiming at harming the systems.

This year, we also saw some incidents of cable theft, where copper is very lucrative on the underground market. People steal cables, but in many instances they cut off fibre cables by mistake, thinking they contain copper.

But overloads followed by power cuts caused most impact though. And this is important, showing that the electronic communications depend heavily on the power supply sector.

Could you say something about access to the emergency service number 112?

-Yes, in about 40% of the incidents, there was an impact on the possibility to reach the emergency services over 112. This can of course potentially be extremely serious, and we must remember behind the technology, we are talking people, real people, and potentially about life and death.
Yet, at least for mobile communication, there is an emergency roaming scheme in place, where you can use a guest network for free if your network is down. Providers are obliged by law to participate and to transfer 112 calls to the emergency services. We do not know the actual consequences of not being able to reach the emergency services when they occurred, we do not know that level of granularity of detail of the actual accidents, but they could be fatal if something falters.

-In that sense, it is important to bear in mind that every life counts. This emergency call can be from a pregnant woman, or someone injured in the woods, or at sea, or by any kind of emergency, when you need to have access to emergency services in a dark, stormy night, which causes the failure. That is why resilience and robustness of these systems is needed. That is why we are doing this work, by studying the incidents, to improve this robustness. Just when you need it the most, you cannot access this emergency service and make that crucial call, to save a life. So, this is potentially serious, and therefore concerning, that this traffic in particular is so frequently occurring among the incidents.

Out of the 79 incidents reports, almost 40% of the incidents affected the possibility of dialling the emergency number "112"

Is the figure of 79 major incidents in Europe in 2012 not rather low?

I agree; we would have expected more. We know there are more incidents. The more incidents that are known, the more accurate analysis can be made. So, it is the benefit of all that incidents are reported. So we need to discuss about the thresholds, with the NRAs, to refine them even further, so that more reporting is done of actual incidents, as to get a better and more accurate picture of the situation.

What is the total number of users affected?

-What is the total figure is a tricky question. One user can be a subscriber to many services. Therefore you cannot give a fully accurate number. You have to do assumptions. If you have an incident affecting mobile telephony for 300.000 users, and affecting fixed telephony for 100.000 users, it would be very difficult to distinguish how many users were affected in total from this one incident.

-Yet, we can discuss user connections, one user can have several services, and they may all go down. If we speak about user connections, then the figure could be as high as 154.000.000 user connections affected by these 79 reported incidents. But this figure again, has to be taken with great caution, and is only indications, and you have to separate between users, and user connections, as I explained.

So what do the National Regulatory Authorities (NRAs) report?

-They have to report all incidents that they have received from the providers that have reached a certain threshold in terms of affected users and duration for each service.

These thresholds have been agreed upon between ENISA and an expert group of NRAs. So, for example, if an incident lasts more than 1 hour, and the percentage of users affected is more than 15% of the national user base for that particular service, they must report; if it lasts more 2 hours and affected users are more than 10 %, the incident is also reportable, in a falling scale.

-This means it is only the most significant incidents that are passing the thresholds. Obviously, there are other incidents occurring that the NRAs get reports of, as well as incidents not reported to the NRAs. The reports that finally reach ENISA are only the major ones. So, we only show the overview of the major incidents. As such they give us indications, patterns and averages based on the big incidents.

-More in detail, the NRAs should report incidents affecting the following communication services and networks:

- Fixed telephony
- Mobile telephony
- Fixed Internet access
- Mobile Internet access
- NRAs may also report about incidents affecting other types of services
- NRAs should report security incidents, with significant impact on the continuity of supply of electronic communications networks or services

Interview by Ulf Bergström, ENISA.

Background:

Press release

Full report

Article 13a of the EU legal framework for electronic communications, clarifies:

- Providers of public electronic communications networks and services should take measures to **guarantee security and integrity** of their networks.

- Providers **must report to competent national authorities about significant breaches of security or integrity.**
- National Regulatory Authorities should notify ENISA and national authorities abroad when necessary, for example in case of incidents with cross-border impact.
- Annually, National Regulatory Authorities should submit a summary report to ENISA and the European Commission (EC) about the incidents.