Interview – Pascal Manzano

ENISA Security Policy Expert Pascal Manzano is the editor of the recently launched ENISA report on resilience of communication networks. The report is based on a study of network operators across the EU conducted by IDC.

Pascal, what is the background for this report by ENISA and what where some of the findings?
This is a first step in a multi-year program to enhance communication network resiliency in the EU looking at regulations, technologies and industry practices. This study presents a survey of network service providers across the EU with regard to the measures they have applied to ensure network resiliency. The availability of networks, services and business continuity is of major concern for all business actors and consumers alike across Europe and the study shows that there is over 99.9 % availability which might not be say much to some of us, but translated into time this means only 10 hours downtime a year.

What are the operators doing in terms of resiliency?
One reassuring finding of this study was that the operators are taking network resiliency very seriously. Overall, there is a maturity in the operators network and risk management, but there are still improvements that can be made).

What is the importance of resiliency to businesses and end-users?
The survey shows that operators are providing availability and resilience. However the distance between operators and end-users is generally constisting of only one line. This so called “last mile” creates a possible vulnerability on resilience. It is a competitive market and more lines would create costs that has to be paid for. It is important for end-users to take other aspects than price into consideration such as security, availability and filters when choosing an ISP (Internet Service Provider). A comparison could be made with the automobile industry where increased security in cars often leads to an increase in their price.

The same applies to many SME businesses, who also need to consider these other aspects. Companies are offering more and more services and products over internet today. This together with the increase in bandwidth and new applications makes it even more important to secure network resiliency.

What challenges do you see for improving network resiliency in the future?

There are two important aspects when considering improving network resiliency. The first concerns the complexity of networks. Operators today are mixing more services within their networks: mobile and fixed communication, as well as data. The technology for managing their networks as well as the more complex services makes it very hard to get a complete understanding of the entire network. This also means that it makes it harder to be aware of the risks and to be able to manage the effects of network failures.

The other aspect concerns third-parties dependencies. Network operators are in many cases not installing or managing their networks themselves and how the operators are connected with each other, in so called internet exchange points will play an important role for network resilience.

In terms of third-parties dependencies another important issue is the terms in the service level agreements between the operators, meaning that even if one operator has a secure network, parts of the network are managed by another operator who needs to be at the same level, which is an aspect that needs to be taken into account by the operators.

Full report:

http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_network_provider_measures_on_resilience.pdf

FAQ:

http://www.enisa.europa.eu/doc/pdf/faq_resilience.pdf