Club R2GS

Workshop for the European chapters of Club R2GS (20 January 2015 – 7th International Forum on Cybersecurity – Lille)

Towards a standardised pan-European approach to SIEM

Despite pan-European efforts at regulation and harmonisation of law, the world of cybersecurity remains largely compartmentalised in the European Union's 28 member states, especially with respect to operational management of security issues. This long-standing state of affairs is of course due to the sovereign dimension of a country's precise awareness of the threats and attacks it faces and its means of defence. However, it is also a product of the industry's often very nation-specific character.

One of the crucial themes in operational management of security issues today is the detection of security incidents. However, detection rates for the stealthiest incidents are often extremely low, while their impact on organisations and companies can be considerable. In spite of comprehensive initiatives in the last few years, mobilisation of organisations & companies remains quite lacking, producing frequently evident frustrations within Cybersecurity communities in many countries. But highly innovative approaches have recently emerged to change this situation. These approaches are being implemented within certain members of the European community of users of Club R2GS, which today comprises 6 chapters in 6 different countries. These approaches are organised around 2 main axes, which are:

- On the one hand, the use of a common security event classification model and associated operational indicators with up-to-date statistics that allow accurate benchmarking of security levels, and
- On the other hand, the establishment of better dialogue with management by effectively raising executive committees' awareness before incidents occur. The pioneering quantitative approach of the former axis can firmly support the latter.

The main contribution of the 1st axis is a set of 5 new standards (known as ETSI GS ISI-00x) that cover all aspects of detection and occupy a middle ground between a general model and the often very technical standards in the field of operational management of security issues. The standards thus play the key role of a bridge between the world of governance and the world of Cybersecurity experts. Their increasingly successful application (in particular, the full set of 94 indicators) stems from a combination of factors such as: simplicity and ease of understanding; a solid and well-developed methodology; an approach enhanced by ISO JTC 1/SC 27, supported by the very active Club R2GS community, rooted in a large user base and subject to continuous improvement over the last 5 years; and, lastly, 8 compelling practical uses at the crossroads of expertise and management. Exchanges within the profession include a use related to gathering and sharing experiences, which has allowed roughly 40 SOC experts to capitalise on best practices in detection for 20 different types of incidents. The initiative is the only one of its kind in Europe to date.

This quantitative view of the company's level of protection and the progress it allows, however, proves very inadequate nowadays if the proposed approach involves only security and IT professionals. Two key figures can be drawn on to support these claims and on their own illustrate the limitations of approaches that rely too heavily on specialists and demonstrate the need to broaden the approach to include a company's entire management (2nd axis of the approach):

- 70% of security incidents are made possible through the exploitation of critical software vulnerabilities or by basic technical or behavioural non-compliance (for example, the weak passwords cited in the latest Verizon Data Breach Investigation Report);
- 70% of all security incidents (internal or external) involve negligent, deviant or malicious behaviour within companies (for example, web browsing).

These figures relate to the field of user awareness raising. This has been considered a subject in itself for several years within the profession, but, unfortunately, its effects have fallen far short of companies' expectations and hopes. Because a radical paradigm shift with a fundamentally refashioned approach to cybersecurity is genuinely necessary. Its essential components could be summed up as follows:

- Getting the company's executive committee involved by having it treat cyber risks as it treats the other major risks it must face, so that the entire management becomes more concerned;
- Raising awareness and effectively getting management involved in Cybersecurity by making new appeals to personal motivation and attempting to answer the fundamental question of « Why? » (« Why should I be concerned about cybersecurity? ») before « How? » and « What? »;
- Among Cybersecurity managers, demonstrating a willingness to change and more carefully consider needs related to business and ease of use, and to simplify associated IT processes as much as possible.

The two axes of this extensively overhauled approach to cybersecurity have the further advantage of being transnational, which allows them to be compatible with both potential nation-specific policies and major international standards (especially ISO 27000 and COBIT). This is why they are being progressively adopted throughout Europe, in particular thanks to the efforts made by the different Club R2GS chapters to promote their adoption.

And it is logical to address this subject in a dedicated workshop (20 January at 2:00 pm) within the framework of an event like the FIC, which has made cross-European targeting one of its priority objectives.

by Gérard Gaudin (Chairman of Club R2GS France and of Club R2GS Europe)