Industry program panel

Feltus, Christophe

Published in:
SIN 2013 - Proceedings of the 6th International Conference on Security of Information and Networks

DOI:
10.1145/2523514.2527023

Publication date:
2013

Document Version
Early version, also known as pre-print

Industry Program Panel

Christophe Feltus
Public Research Centre Henri Tudor,
Luxembourg
christophe.feltus@tudor.lu

The security of the information owned by the industries is judged as the main concern of these industries' managers, even more than the possibility of the euro zone's breakup or any natural disaster. This statement has been reported by the recent « *Global State of Information Security Survey 2013* » published by PwC and CIO Magazine. This observation must be analysed in parallel to a continuous gowning of the worldwide investment in information security, which has been estimated by PwC, up to 500 billion dollars. Despite the great importance given in the information security, it is noted that 71 percent of these managers continue, in the meantime, to trust their information security system, although only 8 percent of them really possess an organisation adapted to the new information risks.

This survey from PwC and CIO Magazine is one of a few which highlights the importance of addressing security in the industry, through a consistent and integrated manner to efficiently handle the risk that threatens the industry exposure to a huge financial impact. In the 2011 study « *Global Risk Management* » published by Accenture, it was equivalently identified that "risk management is now more closely integrated with strategic planning and is conducted proactively, with an eye on how [risk management] capabilities might help a company move into new markets faster or pursue other evolving growth strategies".

In this perspective, analysing the potential security risk appears to always increase in complexity due to the new information system possibilities and ongoing development of the critical infrastructures in the sectors such as finance, healthcare, transport, energy or army. One of the reasons generating this growing of complexity and sophistication partially stays in the openness of the solutions and in the disappearance of borders that long ago served as safeguard between the information owned by the industry and its ecosystem. An example of this is the adoption of the cloud-based services and the parallel sharp increase in attacks against these services (dedicated to private or industrial usage). Another reason that explains this increase of complexity of the risk appraisal is the industrialisation of the cybercrime activities, which, as reported in the 2010 report « *Cybercrime: a clear and present danger. Combating the fastest growing cyber security threat* » published by Deloitte, tends to be supported by a vigorous and rapidly growing underground economy encompassing hackers, disaffected employees, customers or providers, as well as terrorists. This blurred environment and the high number of possible malicious acts (e.g. fraud, identity or intellectual property theft, system sabotage, data destruction, corporate espionage and so forth) makes it difficult to accurately and definitively address a potential exposure scenario. Beside this evolution of the industry information system environment, we must also stress the continuous expansion of the privacy and confidentiality of the information managed. This sensitivity of the information is also obviously to be considered, in the risk equation, as a significant impact factor.

In view of those considerations, industries and academics are continuously forced to further undertake partnerships and collaborations in current and new researches in the various areas of the information security, i.e. technology, application and management. Many surveys frequently highlight the impact resulting in the successful adoption of academic issues through the market. This is for instance the case of the 2010 *« Economic Analysis of Role Based Access Control Final* » report [1] which has demonstrated that, in the field of the identity and access management, the use of roles in American companies with more than 500 employees has significantly grown since 1994. It has additionally proven that the number of employees which have their permission managed using roles has increased from 2.5 percent in 1995 up to 40.5 percent in 2009. Additionally, 84 percent of them agree that the use of roles improved the efficiency of maintaining the organisation's access control policy. Another initiative, which has been initiated in early 2011, is the joint project between members from the Architecture, Security and ArchiMate Forums, which have begun a cooperative initiative to "integrate security into a re-structured version of the TOGAF specification - the project being named TOGAF next (TN), and Security Forum contributions being driven in a TOGAF next security project (TNSP). After the completion of this project, the ArchiMate Forum members intend to incorporate the relevant TNSP security information into the ArchiMate standard" [2].

Industrial track research papers have a strong focus on establishing safeguards to defend the industry's resources from crimes, thefts, corruption and any form of destruction, on defining the responsibility and managerial structure for the organisation of the information security, and on defining infrastructure for the monitoring and deployment of counter measures for minimising the occurrence and asperity of security incidents, thereby ensuring, amongst others, the continuity of the commercial and production activities. Accordingly the Industry track of the 6th International Conference on Security of Information and Networks (SIN 2013) provides a high quality international forum for presentations of research and applications of security in information and networks, with the ambition to sustain and enhance the collaboration between researchers and actors of the economy, from high qualified technicians to skilled managers.

SIN '13, Nov 26-28 2013, Aksaray, Turkey
ACM 978-1-4503-2498-4/13/11

REFERENCES

[1] Alan C. O'Connor and Ross J. Loomi. Economic benefits of role based access control analyzes economic value of rbac for the enterprise and for the national economy, and provides quantitative economic benefits of rbac per employee for adopting firms. 2011

[2] http://www.opengroup.org/projects/security/archisec/