

Instrumente manageriale în asigurarea securității sistemelor informatice

Costel CIUCHI, Angelica BACIVAROV

EUROQUALROM Laboratory, ETTI, University „Politehnica“ of Bucharest, Romania
ciuchic@yahoo.com

Abstract

The risk management in information security area involves a range of economic issues, with direct implications in the development of decision-making process in an organization. Operationally, cost-benefit analysis is a common practice to justify investment in security. This article makes an analysis of methodology to quantify the security with economic cost-benefit models (ROI – Return on Investment, NPV – Net Present Value and IRR – Internal Rate of Return). The models are analyzed in terms of possible uses, popularity and complexity.

Keywords: security, risk, decision, management, cost-benefit analysis

References:

- [1] Gerald Kovacich, Edward Halibozek, „Security Metrics Management: How to Manage the Costs of an Assets Protection Program“, Butterworth-Heinemann, 2006.
- [2] Martin Kutz, „Controlling der Information Security, chapter 03710, Number 32, Aktualisierung September 2011 in Praxiswissen IT-Sicherheit: Praxishandbuch für Aufbau, Zertifizierung und Betrieb. TUV Media – Dieter Burgartz and Ralf Rohrig, 19 edition, 2011.
- [3] COM (2007) 267, European Commission, Towards a general policy on the fight against cyber-crime, May 2007.
- [4] DETICA and Office of Cyber Security and Information Assurance, „The cost of cyber-crime“, February 2011.
- [5] National Institute of Standards and Technology (NIST), „Special Publication 800-30: Risk Management Guide for Information Technology Systems“, July 2002.
- [6] B. Blakley, E. McDermott, and D. Geer, „Information security is information risk management“, Proceedings of NSPW, Cloudfroft, New Mexico, USA, 2002.
- [7] J. R. Conrad, „Analyzing the Risks of Information Security Investments with Monte-Carlo Simulations“, IEEE Computer Society, 2005.
- [8] Rebecca T. Mercuri, „Analyzing Security Costs“, Communications of the ACM, 2003.
- [9] A. L. Gordon, P. M. Loeb, „The economics of information security investment“, ACM, 2002.
- [10] S. E. Schechter, „Quantitatively differentiating system security“, The first workshop on economics and information security (WEIS), 2002.
- [11] Michael E. Whitman and Herbert J. Mattord, „Principles of Information Security“, Thomson Course Technology, 2008.
- [12] Thomas R. Peltier, „Information Security Risk Analysis“, CRC Press, 2005.
- [13] M. Neuhaus, „Corporate Finance“, Swiss Federal Institute of Technology Zurich, 2008.
- [14] A. L. Gordon and R. Richardson, „The new economics of information security“, Information Week, 2004.

[15] R. Bojanc and B. J. Blazic, „Towards a standard approach for quantifying an ICT security investment“, Computer Standards & Interfaces, 2007.