Acta Universitatis Bohemiae Meridionales
The Scientific Journal for Economics, Management and Trade
České Budějovice, 2009, XII, (3) s. 93-98

THE PROPOSAL OF SOFTWARE DEVELOPMENT AND ACQUISITION METRICS BASED ON ISO/IEC 27001 STANDARD

L. Beránek, R. Remeš

Abstract

The implementation and operation of efficient information security management systems (ISMS) according to the ISO/IEC 27001 standard involves a number of steps, among others implementation and operation of appropriate processes, policies and objectives. The crucial issue is the correct definition of the metrics for measurement of the effectiveness of established processes and established controls. The paper describes some practical metrics for ISMS processes review but primarily deals with the metrics for the security category "Security in development and support processes" from the security control clause "Information systems acquisition, development and maintenance processes" (ISO/IEC 27001, ISO/IEC 27002). Judged by the authors' research and experience, organizations often concentrate mainly on other security categories (Correct processing in application, Cryptographic controls, Security of system files) from the security control clause "Information systems acquisition, development and maintenance processes" (ISO/IEC 27001, ISO/IEC 27002). The aim of this paper is to refocus on the necessity to define appropriate metrics for all processes (controls) corresponding to the "Information systems acquisition, development and maintenance" security clause.

Key words: Security metrics, information security, ISO 27001, ISMS, software development

Abstrakt

Příspěvek stručně popisuje zavádění systémů řízení bezpečnosti informací (ISMS) dle ISO 27001 se zaměřením na metriky v oblasti vývoje a pořizování software. Vzhledem k tomu, že při zavádění ISMS se jedná o nastavení řídicích procesů, je důležitou otázkou stanovení bezpečnostních metrik pro měření účinnosti a efektivnosti procesů a přijatých opatření. Příspěvek se zaměřil na metriky pro základní oddíl „Nákup, vývoj a údržba informačního systému" (ISO/IEC 27001, ISO/IEC 27002) a zejména na oblast „Bezpečnost procesů vývoje a podpory". V této oblasti se, podle zkušeností autorů, většina firem soustředí spíše na opatření z ostatních oblastí (tedy z oblastí „Bezpečnostní požadavky systémů", „Správné zpracování v aplikacích", „Kryptografická opatření" a „Bezpečnost systémových souborů"). Návrh metrik, které by byly smysluplné a umožnily kontrolovat a řídit procesy implementované v rámci systému řízení bezpečnosti informací, není jednoduchý. Cílem příspěvku na základě výzkumů a zkušeností s návrhem ISMS pro konkrétní organizace je ukázat, že je nutné definovat vhodné metriky pro všechny procesy (opatření) odpovídající všem oblastem oddílu ISO/IEC 27001 (ISO/IEC 27002) „Nákup, vývoj a údržba informačního systému", a dále ukázat, jak je možné tyto metriky konstruovat.

Klíčová slova: Bezpečnostní metriky, bezpečnost informací, ISO 27001, ISMS, vývoj software

Reference

[1] *Český normalizační institut*. 2004 [ref. 2009-03-20]. Available on: http://domino.cni.cz/NP/NotesPortalCNI.nsf/key/hlavni_stranka?Open.

[2] Are you ready for a BS ISO/IEC 27001 ISMS audit?. *British Standard Institution Publications*. 2008 [ref. 2009-03-20]. Available on: http://www.standardsuk.com/shop/pro ducts_list.php?keyword=BIP%200072:2005&searchtype=quicksearch&textsearchtype=BSi.

[3] Howard, M., Pincus, J., Wing, J. Measuring Relative Attak Surfaces. 2003 [ref. 2009-03-20]. Available on: http://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf

[4] Manadhata, K., Wing, J. Measuring a System's Attack Surface. 2004 [ref. 2009-03-20]. Available on: http://reports-archive.adm.cs.cmu.edu/anon/2004/ CMU-CS-04-102.pdf.

Contact address – Kontaktní adresa

Ing. Ladislav Beránek, CSc.
Mgr. Radim Remeš

Jihočeská univerzita v Českých Budějovicích
Ekonomická fakulta
Katedra aplikované matematiky a informatiky
Studentská 13

370 05 České Budějovice
E-mail: beranek@ef.jcu.cz
Tel. 389 032 511
E-mail: inrem@ef.jcu.cz
Tel.: 389 032 461