UNIVERSITY OF TARTU
FACULTY OF MATHEMATICS AND COMPUTER SCIENCE
Institute of Computer Science
Cybersecurity Curriculum

Christopher Helbig

An Experience Report of Eliciting Security Requirements from Business Processes

Master's Thesis (30 ECTS)

Supervisor: Dr. Raimundas Matulevicius

Tartu 2014

An Experience Report of Eliciting Security Requirements from Business Processes

Abstract:

Small and Medium Sized Enterprises struggle to find strategies to achieve a high level of information security or are unaware of the risks posed by information technology. A lack of finance and IT departments that miss an information security officer increase the risk of exploited vulnerabilities. The alignment of Business Process Management and Security engineering manifested in the Security Requirements Elicitation using Business Processes approach provides a solution of this sector wide issue by introducing Security Risk-oriented Patterns applicable also for Business analysts. Patterns that are based on contextual areas illustrate business assets, vulnerabilities and risk treatment in form of security requirements. This is achieved by using the Business Process Model and Notation 2.0 modeling language and specifically engineered extensions which add the IT security domain. Outcome of this bridging is an applicable solution to elicit security requirements. Core of this thesis is the pattern application to measure their performance in a German SME. After business assets and security objectives were set, several pattern occurrences have been identified that resulted in a number of security requirements. Implementation abilities and usefulness with regards to the company underlined strong pattern performance. Moreover, a new pattern has been developed by using the Information System Security Risk Management Domain Model. Finally, the inclusion of prioritization and inspection techniques from the Security Quality Requirements Engineering methodology is suggested and extensions from the theorem of organizational configurations that enable further automation of SREBP. These modifications result in an approach that increases the security of Small and Medium Sized Enterprises.

Keywords: Small and Medium Sized Enterprises; Business Process Management; Security Requirements Elicitation using Business Processes; Security Risk-oriented Patterns; security requirements; pattern occurrences; Information System Security Risk Management Domain Model

Praktika Aruanne äriprotsessidest tulenevate ohutusnõuete esile kutsumise kohta

Lühikokkuvõte:

Väikesed ja keskmise suurusega ettevõtted näevad vaeva, et leida strateegiaid saavutamaks kõrgetasemelist infoturvet. Tihti ei ole need ettevõtted teadlikud infotehnoloogiaga seonduvatest riskidest. Lisaks suurendab haavatavuse riski finants- ja IT osakondade vähesus, kellel ei ole oma teabeturbe ametnikku. Äriprotsesside juhtimise ning joondamine, mis omakorda avaldub turvalisuse vajaduste esiletoomises kasutades äriprotsessidepõhist lähenemist, pakub sellele sektoripõhisele teemale oma lahenduse, võimaldades juurutada turvalisuse riskidele orienteeritud mudeleid ka ärianalüütikute jaoks. Kontekstuaalsetel valdkondadel põhinevad mustrid illustreerivad ettevõttevarasid, haavatavust ja riskikohtlemist turvanõuete kujul. See saavutatakse kasutades äriprotsesside mudelit, *Notation 2.0* modelleerimiskeelt ning spetsiaalselt projekteeritud lahendusi, mis lisanduvad IT turvalisuse valdkondkonnale. Selle tulemuseks on kohaldatav lahendus, mis kutsub esile turvanõuded. Selle uurimuse keskmes on mustrite rakendumine, mõõtmaks nende sooritust saksa SME-s. Ärivahendite ja ohutusalaste eesmärkide määramise järel identifitseeriti mitmed mustri esinemised, mis kulmineerusid mitmete ohutusnõuete määramisega. Rakendamise oskuste ja kasutatavusega seoses ettevõttega, tõi esile väga selge mustrite esinemise. Lisaks arendati eelnevaga seoses uus muster kasutades informatsioonisüsteemi turvariski juhtimise domeeni *(Information System Security Risk Management Domain)* mudelit. Lõpetuseks soovitab autor käesolevas uurimuses prioritiseerimise ja inspektsiooni meetodite kaasamist ohutuskvaliteedi nõuete tehnika metoodikast ning organisatsioonilise koosseisu teoreemi laiendust, mis omakorda võimaldab SREBP-i täiendavat automatiseerimist. Need muudatused toovad kaasa käsitluse, mille alusel suureneb väikese ja keskmise suurusega ettevõtete turvalisus.

Märksõnad: väiksed ja keskmise suurusega ettevõtted, äriprotsesside juhtimine, ohutusnõuete esilekutsumine äriprotsesside baasil, ohutusriskialased mustrid, ohutusnõuded, mustri esinemised, informatsioonisüsteemi turvariski juhtimise domeeni mudel.

Non-exclusive licence to reproduce thesis and make thesis public

I, Christopher Helbig (12.05.1987),

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to:

1.1. reproduce, for the purpose of preservation and making available to the public, including for addition to the DSpace digital archives until expiry of the term of validity of the copyright, and

1.2. make available to the public via the university's web environment, including via the DSpace digital archives, as of **13.06.2064** until expiry of the term of validity of the copyright,

An Experience Report of Eliciting Security Requirements from Business Processes

supervised by Dr. Raimundas Matulevicius

2. I am aware of the fact that the author retains these rights.

3. This is to certify that granting the non-exclusive licence does not infringe the intellectual property rights or rights arising from the Personal Data Protection Act.

Tartu, **26.05.2014**