Simo: Security Incident Management Ontology

Pâmela Carvalho da Silva[1], Leonardo Lemes Fagundes[1]

Universidade do Vale do Rio dos Sinos (UNISINOS)
CEP 93.022-000 – São Leopoldo – RS - Brasil

Resumo. *Os incidentes de segurança da informação apresentam características comuns, bem como variações quanto aos ataques, sua complexidade e sofisticação. Isto requer profissionais capacitados para desempenhar ações e atividades relacionadas a identificação, tratamento e prevenção de incidentes. O trabalho proposto apresenta uma abordagem para auxiliar e apoiar a capacitação de profissionais com o uso de uma ontologia de domínio para a gestão de incidentes de segurança da informação baseada na norma ISO/IEC 27035:2011.*

Abstract. *The information security incidents present common features, but also variations in the attacks, its complexity and sophistication. That requires trained professionals to perform actions and activities related to identification, treatment and prevention of incidents. The proposed project presents an approach to assist and support the training of professionals using a domain ontology for incident management of information security, based on ISO / IEC 27035: 2011.*

1. Introdução

O cenário de ataques expande-se em quantidade, diversidade, complexidade, sofisticação e subversividade (Mccarthy, 2014). Dentre as causas, destacam-se a constante e crescente dependência de sistemas e tecnologias da informação; a popularização de novas tecnologias; e a motivação e ousadia dos atacantes.

Este cenário, caracterizado pelo alto número de incidentes e pela sofisticação dos novos ataques, exige profissionais capacitados. A sofisticação das ameaças requer a estruturação de habilidades referentes a prevenção, identificação e tratamento (Torres, 2014). A gestão de incidentes (GI) surge como um importante componente da SI e pode ser estabelecida para o desenvolvimento e apoio às habilidades supracitadas (Cichonski, et al., 2012.).

O estabelecimento da capacidade de GI requer a definição de procedimentos, atribuição de funções e responsabilidades, infraestrutura, ferramentas e materiais de apoio adequados e equipe qualificada e treinada para a realização de um trabalho consistente, confiável, de alta qualidade e capaz de ser repetível (Killcrece, 2005). Quanto aos procedimentos, cabe destacar que o processo de GI envolve atividades relacionadas a coordenação, suporte, avaliação de incidentes e tratamento de incidentes, que por sua vez é composto por diversas fases: detecção, triagem e resposta. Para desempenhar tais atividades são exigidos conhecimentos de múltiplas áreas, ademais muitas das atividades envolvidas são de natureza não determinística (Mundie e Ruefle, 2012). Eis, portanto, um contexto multidisciplinar e complexo, que resulta em muitos desafios. Entre os desafios, destacam-se a capacitação de profissionais para o tratamento de incidentes a partir de conhecimentos prévios do domínio da GI. (Torres, 2014) As dificuldades relacionadas associam-se a

fatores como a difícil formalização dos conhecimentos tácitos dos envolvidos (Mundie e Ruefle, 2012), um desafio da área que não limita-se ao domínio da GI.

O trabalho propõe o desenvolvimento de uma ontologia para o domínio da gestão de incidentes de SI baseada na norma ISO/IEC 27035:2011 e objetiva auxiliar na capacitação de equipes de reposta a incidentes. São referências normativas adicionais as normas ISO/IEC 27001:2013, ISO/IEC 27002:2005 e ISO/IEC 27005:2008.

2. Trabalhos Relacionados

Os trabalhos a seguir relacionados à ontologias e à GI são apresentados e comparados ao proposto (Tabela 1). São utilizados os seguintes critérios de comparação: (i) classificação (vocabulário, tipo de ontologia, taxonomia etc); (ii) referências; (iii) registro de metodologia para construção da ontologia (iv) registro de metodologia para avaliação da ontologia e (v) disponibilidade para a comunidade/publicação.

- Martimiano e Moreira (2005): ontologia que objetiva permitir a correlação de incidentes de SI de diferentes fontes e facilitar a gestão do conhecimento propondo vocabulário único de termos e relações fundamentado no documento *Taxonomy of the Computer Security Incident (TCSI)* de Howard e Longstaff. Não exemplifica a referida correlação.
- Blackwell (2010): ontologia focada na etapa de análise de incidentes e fundamentada no *TCSI* - por ater-se a este, desatende o atual cenário da GI.
- Mudie e Ruefle (2012): *Body of Knowlodge* para GI que visa a possibilitar uma definição da área de conhecimento; padronizar competências, vocabulários e processos; facilitar a criação de um repositório; orientar a descrição de requisitos, formações e competências exigidas a profissionais; e propiciar análise/melhoria do processo de GI nas organizações. Baseia-se em dez documentos da área de SI e/ou GI. Não elege uma metodologia específica para construção, mas lista suas etapas.

Tabela 1. Comparativo trabalho proposto e trabalhos relacionados

Trabalhos	Classificação	Ref.ISO/IEC 27035/2011	Metodologia construção	Metodologia avaliação	Publicada
Martimiano e Moreira(2005)	Não especificado	Não	Sim	Não	Não
Blackwell (2010)	Não especificado	Não	Não	Não	Não
Mudie e Ruefle (2012)	Body Of Knowlodge	Não	Não se aplica	Não se aplica	Não
SIMO	Ontologia de Dominio	Sim	Sim	Sim	Sim

Dos trabalhos relacionados, a ontologia proposta distingue-se quanto à referência primária, a norma ISO/IEC 27035:2011, à disponibilidade aos usuários via Web Protégé, aos métodos avaliativos e, sobretudo, ao objetivo de auxiliar a capacitação de equipes de GI.

3. Trabalho Proposto - Ontologia

De acordo Rautenberg et al. (2008), há várias metodologias para o desenvolvimento de ontologias, não há consenso quanto a um padrão; recomenda-se, a combinação de

metodologias. A partir das metodologias de Noy e Mcguinness (2001), Sure et al., (2004) e Bouiadjra e Benslimane (2011), elaborou-se a metodologia a seguir, conforme figura 1.

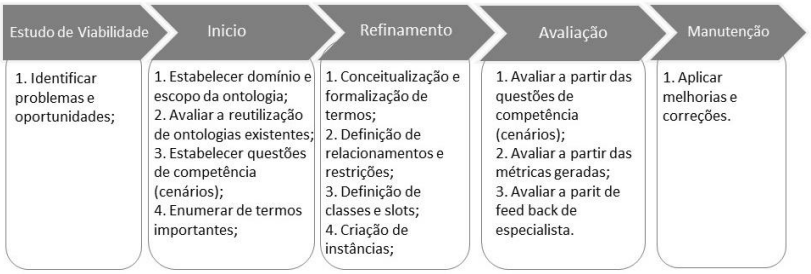

Figura 1. Metodologia Utilizada

Conforme Noy e Mcguinness (2001), a ontologia deve responder a cinco questões: Qual domínio a ontologia abrange? Representação do conhecimento de GI necessários a equipes de resposta; A ontologia será utiliza para quê? Auxiliar na capacitação de equipes de resposta; Qual questão a ontologia deve ser capaz de responder? Deve ser capaz de fornecer informações relacionadas a um incidente de SI, como sua categoria, classificação, causa ou ameaça, ativos envolvidos, impacto do incidente, ações de resposta, vulnerabilidade(s) e atacante ou perpetrador.

A partir da enumeração de termos, mapearam-se os termos e suas relações. Após o refinamento, consolidou-se uma visão da ontologia proposta, conforme figura 2. Cada uma das classes definidas apresenta subclasses, propriedades e instâncias considerando as normas utilizadas como referências.

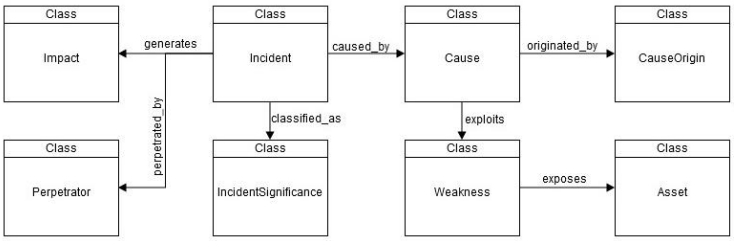

Figura 2. Mapeamento ontologia com classes e propriedades de objetos

As figuras 3 e 4 descrevem a ontologia proposta a partir da classe Incidente, expondo algumas das propriedades de dados e propriedades de objetos. A ontologia conta ainda com outras 11 propriedades de objetos e 11 propriedades de dados (4 de primeiro nível e 7 de segundo nível), totalizando 16 e 25 respectivamente.

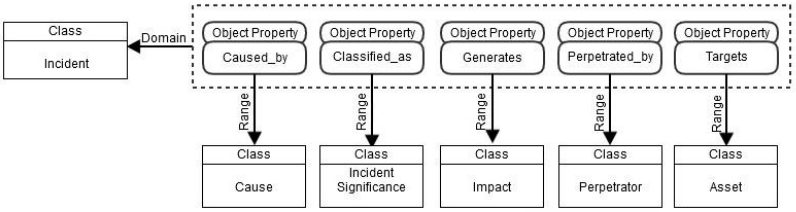

Figura 3. Descrição Ontologia Parcial - Classe Incidente e Objetos

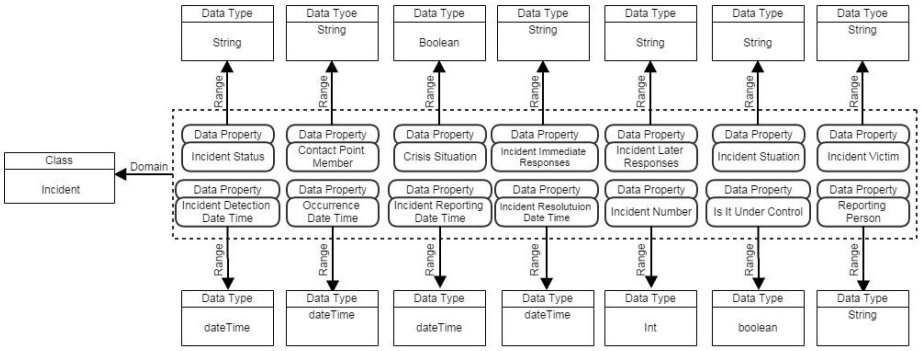

Figura 4. Descrição Ontologia Parcial - Classe Incidente e Dados

4. Considerações Parciais

Nesse momento, objetiva-se a criação de cenários de incidentes adicionais para avaliar a competência da ontologia, além da submissão do trabalho à avaliação de profissionais de equipes de resposta a incidentes, no intento de verificar sua efetividade. A geração de um protótipo de software para GI a partir da ontologia também é uma proposta de trabalho futuro. A ontologia está disponível para consulta e utilização em http://webprotege.stanford.edu/ pelo nome SIMO.

Referências

Blackwell, C.(2010) "A security ontology for incident analysis", Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence research, p. 1-4.

Bouiadjra, A., B., E Benslimane, S. (2011) "FOEval: Full Ontology Evaluation -Model and Perspectives", IEEE, Tokushima, p. 464-468

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012) "Computer Security Incident Handling Guide." Recommendations of the NIST, Gaithersburg,

ISO/IEC 27035 (2011) "Information technology – Security techniques – Information security incident management".

Killcrece, G. (2005) "Incident Management", SEI CMU, Pittsburgh, Pennsylvania.

Martimiano, L. A. F.; Moreira, E. Dos S. (2005) "An OWL-based Security Incident Ontology".

Martimiano, L. A. F.; Moreira, E. Dos S. (2006) "The Evaluation Process of a Computer Security Incident Ontology", Ribeirão Preto.

Mccarthy, N.K. (2014) "Resposta a Incidentes de Segurança em Computadores: Planos para Proteção de Informação em Risco", Porto Alegre, Bookman.

Mundie, D. A., E Ruefle, R. (2012) "Building an Incident Management Body of Knowledge", In: ARES, Washington , p. 507–513

Noy, F. N., E Mcguinness, D. L. (2001) "Ontology development 101: a guide to create your first ontology"

Rautenberg, S., Todesco, J., Steil, A. E Gauthier, F. (2008) "Uma Metodologia para o Desenvolvimento de Ontologias", Guarpuava, Paraná, v. 10, n. 2, p. 237-262

Sure, Y., Staab, S. E Studer, R. (2004) "On-To-Knowledge Methodology". Nova York, Springer.

Torres, A. (2014) "Incident Response: How to Fight Back", Survey Incident Response 2014, SANS Institute.

