Um estudo do alinhamento entre sherwood applied business security architecture (sabsa) e iso 27002

SÉRGIO HENRIQUE OLIVEIRA PEREIRA
Centro Paula Souza – São Paulo – Brasil
shopereira@gmail.com

NAPOLEÃO VERARDI GALEGALE
Centro Paula Souza – São Paulo – Brasil
nvg@galegale.com.br

MARÍLIA MACORIN DE AZEVEDO
Centro Paula Souza – São Paulo – Brasil
mmacorin@radial.br

Resumo - Buscando atender a crescente demanda de alinhamento entre Segurança da Informação e negócio, surge a necessidade de um estudo mais aprofundado dos padrões, boas práticas, normas e/ou *frameworks* de mercado para o embasamento de um programa de Segurança da Informação.
Programa esse que trará suporte para a Governança Corporativa, possibilitando que Segurança da Informação deixe de existir na corporação em forma de blocos independentes e seja permeável por toda a ela. Assim, havendo um ganho significativo no melhoramento dos processos internos e externos relacionados à Governança de Arquitetura, Governança de Tecnologia da Informação e Governança Corporativa.

O estudo do alinhamento entre *Sherwood Applied Business Security Architecture – SABSA* e ISO 27002 dará o suporte necessário para o desenvolvimento do programa de Segurança da Informação dentro da corporação bem como fornecerá informações necessárias na mitigação de riscos inerentes ao negócio e também fornecerá indicadores para uma análise dos possíveis benefícios de se possuir Segurança da Informação integrada ao negócio.

Abstract – To attend the high demand of alignment of Information Security and business, a better understanding of standards, best practices, norms and/or frameworks is necessary to serve as base for an Information Security Program.
This program will bring support to the Enterprise Governance, making possible for Information Security to be part of entire corporation and not independent silos. Therefore, a significant improvement of the intern and extern processes related with Architecture, Information Technology and Enterprise Governance.
The alignment study between Sherwood Applied Business Security Architecture – SABSA and ISO 27002 will give us the necessary support to develop an Information Security Program for the corporation that will provide necessary information to mitigate business intrinsic risks and also it will provide key indicators for a better benefit analysis of having Information Security and business aligned.

Palavras-chave: Segurança da Informação, ISO 27002, SABSA, ISO 17799, Governança.

Introdução

Com o aumento crescente da necessidade de alinhamento de Segurança da Informação com os negócios da corporação, surge a inevitável busca por padrões, boas práticas, normas e/ou *frameworks* de mercado para embasar um programa de Segurança da Informação. Assim, buscando apoio e ajuda para o estabelecimento da Governança em Segurança da Informação corporativa.
A grande dificuldade de se estabelecer a Governança em Segurança da Informação nas corporações se dá pelo fato de que Segurança da Informação existe em blocos independentes e não conectados à visão corporativa de negócio. Governança em Segurança da Informação visa exatamente a conexão dos blocos existentes e isolados, permeando assim Segurança da Informação por toda a corporação, havendo um ganho no melhoramento dos processos internos e externos relacionados à Governança de Arquitetura Corporativa, Governança de Tecnologia da Informação e Governança Corporativa.
Para nos ajudar a estabelecer a Governança em Segurança da Informação existem vários *Frameworks* no mercado como CobiT *(Control Objectives for Information and related Technology),* SABSA (*Sherewood Applied Business Security Architecture*), normas como ITIL *(Information Technology Infrastructure Library)* e padrões como *ISO 27002*. Esses já existentes por um bom tempo e com um grau de maturidade satisfatório. A proposta de estudo do alinhamento entre *Sherwood Applied Business Security Architecture – SABSA* e ISO 27002 permitirá a implantação e/ou um controle mais eficaz dos processos relacionados às Governanças de Arquitetura, Tecnologia da Informação e Corporativa. Ainda, contribuirá para a mitigação dos riscos inerentes ao negócio bem como fornecer indicadores para uma análise dos possíveis benefícios de se possuir Segurança da Informação integrada ao negócio.

Metodologia

Dentre os possíveis métodos de pesquisa científica os métodos comparativo e tipológico serão adotados a fim de levantar as semelhanças e divergências entre os dois *framworks* - *Sherwood Applied Business Security Architecture* (SABSA) e ISO 27002 – e também a construção de um modelo ideal que represente o alinhamento entre os mesmos. Esta investigação mapeará os requisitos mínimos necessários para a implantação e/ou controle dos processos relacionados á Segurança da Informação e o negócio.

Como técnica de pesquisa científica será adotada a técnica de observação direta extensiva que através de questionários com questões mistas ajudará na composição de massa de dados para que sejam extraídas informações relevantes para a composição dos requisitos mínimos para a implantação e/ou controle dos processos acima citados.

Pela complexidade das possíveis combinações de requisitos mínimos, em função das respostas dos questionários, a opção por um estudo de caso será explorada. Uma empresa de grande porte na área de seguros será alvo de tal estudo.

O modelo sherwood applied business security architecture - SABSA

SABSA é um modelo e também uma metodologia para desenvolvimento de arquitetura corporativa orientado a riscos bem como usada para a entrega de soluções de Segurança para Infra-estrutura, sempre voltada ao negócio. Publicado pela primeira vez em 1996 em Londres como 'SABSA: *A Method for Developing the Enterprise Security Architecture and Strategy*'. O trabalho desenvolvido por John Sherwood teve como inspiração a ISO 7498-2 de 1989 '*Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*'.

A principal característica do modelo SABSA é que tudo deve partir de uma análise dos requisitos do negócio para Segurança. O processo analisa os requisitos de negócio criando forma de rastreamento das fases através de estratégia e conceito, modelagem, implementação e continuo "gerenciamento e medidas" do clico de vida garantindo que as demandas do negócio sejam preservadas.

SABSA é divido em seis camadas, onde a camada superior é exatamente o estágio de definição dos requerimentos do negócio. A cada camada inferior um novo nível de abstração e detalhe é desenvolvido, passando pela definição conceitual de arquitetura, arquitetura de serviços lógicos, arquitetura de infra-estrutura física e finalmente no nível mais baixo a escolha de tecnologias e produtos.

ISO 27002

A ISO 27002, conhecida anteriormente como ISO 17799 é um código de boas práticas para a Segurança da Informação. Basicamente composta por centenas de controles e mecanismos os quais podem ser implementados.

O padrão em questão, em teoria, estabelece um guia de boas práticas e princípios gerais para iniciar, implementar, manter e melhorar o gerenciamento da Segurança da Informação de um organização. Os controles atuais oferecidos pela ISO 27002 existem com o intuito de endereçar requisitos específicos identificados através de uma avaliação de risco formal. A ISO 27002 também vem para atuar como guia para o desenvolvimento dos padrões de segurança dentro da corporação e práticas efetivas do gerenciamento de segurança.

Com base em documento publicado pelo governo do Reino Unido, se tornou oficialmente um padrão em 1995 quando foi republicado pela BSI como BS7799. Novamente republicado em 2000, desta vez pela ISO, como ISO 17799. Uma nova versão surgiu em 2005 quando, também, foi publicado a ISO 27001.

Referências Bibliográficas

[1] MC Bernardes, E dos Santos Moreira. UM MODELO PARA INCLUSÃO DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO. Disponível em: HTTP://scholar.google.com/url?sa=U&q=http://www.linorg.cirp.usp.br/SSI/SSI2005/artigos/14275.pdf. Visitado em 11/05/2008.

[2] [ISACA a] Executive Summary. ISACA – Information Systems Audit and Control Association & Foundation, 3rd Edition, 2000.

[3] [ISACA b] Framework. ISACA – Information Systems Audit and Control Association & Foundation, 2000.
[4] [ISACA c] Management Guidelines. ISACA – Information Systems Audit and Control Association & Foundation, 2000.
[5] [ISACA d] Control Objectives. ISACA – Information Systems Audit and Control Association & Foundation, 2000.
[6] ABNT – Associação Brasileira de Normas e Técnicas. Tecnologia da informação Código de prática para a gestão da segurança da Informação. NBR ISO/IEC 17799:2005
[7] ENTRUST. Information Security Governance (ISG): An Essential Element of Corporate Governance. April, 2004. Disponível on-line em: http://www.entrust.com/governance/. Visitado em 13/05/2008.
[8] ISO-International Organization for Standardization/ International Eletrotechnical Committee. Information technology- Code of practice for information security management. Reference number ISO/IEC 17799:2005.
[9] IIA-THE INSTITUTE OF INTERNAL AUDITORS. Information Security Governance: What Directors Need to Know. (2001). The Critical Infraestructure Assurance Project. ISBN 0-89413-457-4. Disponível on-line em http://www.theiia.org/. Visitado em 21/05/2008.