III Encontro Internacional de Gestão, Desenvolvimento e Inovação
10 a 13 de setembro de 2019 | Naviraí - MS
III EIGEDIN 2019

SEGURANÇA DA INFORMAÇÃO: enfoque na Cybersecurity

Daniele Almeida do Império,
Universidade Federal de Mato Grosso do Sul,
daniele.a.imperio@gmail.com

Fábio da Silva Rodrigues,
Universidade Federal de Mato Grosso do Sul,
fabiosrod@gmail.com

RESUMO

No seguinte trabalho será apresentado o conceito de Segurança da Informação segundo Araújo (2008) e quais são os princípios que a rege, assim como o conceito de Cybersecurity segundo a Portaria GSIPR nº 45 de 08/09/2009, além de apresentar a ISO 27001, e também mecanismos e ferramentas que visam garantir a segurança dessas informações. Serão mostradas algumas consequências da má gestão da SI nas empresas, e qual a importância de um profissional de SI bem capacitado, bem como o quanto um sistema de segurança pode ajudar a estreitar as relações com os *stakeholders*, aumentando sua confiança principalmente quando se refere ao comércio eletrônico.

Palavras-chave: Segurança; Informação; Gestão; *Stakeholders*; ISO 27001.

O seguinte trabalho tem por objetivo apresentar o conceito de Segurança da Informação/Cybersecurity, assim como os princípios que a rege, também alguns mecanismos de segurança, além de algumas ferramentas que visam fornecer essa proteção. Como a informação está em todos os âmbitos na vida das pessoas, serão apresentados os impactos da segurança da informação (ou da falta dela) em diversos setores, na esfera econômica, social, profissional, na gestão das organizações, além da ISO 27001 que é uma norma internacional que visa à garantia dos princípios da SI nas organizações. A importância desse tema se dá pelo fato de que a população está cada vez mais virtual, centralizando suas vidas em um único aparelho e por isso demanda-se, cada vez mais, conhecer mecanismos de defesa da SI/Cybersecurity.

Segundo Araujo (2008) a SI é a proteção que se tem em relação às informações, sejam elas empresariais ou pessoais, sendo informação definida por conteúdos que possuem valor a esses indivíduos. A Portaria GSIPR nº 45 de 08/09/2009 define Cybersecurity como: "Art. 2º [...] arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus Ativos de Informação e suas Infraestruturas Críticas. […]".

Sendo assim a SI/Cybersecurity visa à preservação das informações das organizações e de seus *stakeholders* através de seus princípios (Confidencialidade, Integridade, Disponibilidade, Autenticidade), como também garantir a continuidade dos processos operativos da empresa em caso de serem *hackeados* ou tiverem algum incidente, diminuindo assim os efeitos deste infortúnio, seja na parte financeira, em sua imagem ou em seu processo operacional.

A confidencialidade está ligada a imposição de limites ao acesso a informação, tornando possível esse acesso apenas por pessoas autorizadas pelo dono da informação. A integridade é quando a informação chega ao seu destino completa ou com as características originais estabelecidas, sem quaisquer modificações, tornando-a confiável. Disponibilidade refere-se à garantia de que a informação será passada (estará disponível) as pessoas autorizadas. Autenticidade assegura que a informação provém, de fato, da fonte pronunciada.

Quando se trata de SI existem alguns mecanismos de proteção da mesma tanto no aspecto de controle físico quanto no controle lógico (uso da tecnologia). Controles físicos seriam barreiras que impedem o contato ou acesso direto a informação como, por exemplo,

portas, trancas, paredes, blindagem, guardas etc. Já o controle lógico, impede ou limita o acesso aos locais ou sistemas por meio do uso de tecnologias. Alguns exemplos são a criptografia que é que um conjunto de regras que codifica a informação para que apenas o emissor e receptor possam traduzi-las. Assinatura digital são os dados criptografados associados a um documento, garantindo assim sua integridade; por isso é considerada o tipo mais avançado e seguro de assinatura eletrônica. A certificação atesta a validade de um determinado documento. Já o Honeypot é um *software* que detecta ou impede a ação de *cracker*, *spammer* ou agentes estranhos ao sistema, iludindo-os, levando-os a pensar que estão realmente explorando uma fragilidade do sistema.

Existem algumas ferramentas e sistemas que são utilizadas almejando fornecer segurança. Entre essas, as mais comuns são, os detectores de intrusão que detectam atividades hostis em computadores ou redes. Analisam incidentes ou possíveis violações e comunicam aos administradores da rede. Os antivírus agem detectando, impedindo e removendo *softwares* maliciosos, códigos e vírus que corrompem, destroem dados ou roubam informações. *Firewalls* trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro dessas regras sejam aprovados, enquanto os outros que não se enquadram nessas regras nunca chegam ao destino final.

Como já pode ser percebido, é de extrema importância às empresas protegerem seus dados visto que quando uma empresa tem o banco de dados invadido, ela tende a perder a confiança investida nela, fazendo com que haja possíveis perdas de clientes e consequentemente de dinheiro. A manchete a seguir é emblemática *"Ações do Facebook caíram 7% após novo vazamento"* (AÇÕES, 2018).

Como também poderá ficar na mão de pessoas mal intencionadas que sequestram os dados para fazer chantagem e assim extorquir as organizações, eles usam, geralmente, *softwares* maliciosos que infectam computadores por meio de anexos de *e-mail*, bloqueando o acesso a esses dados. Segundo Jacobson (2018), através do *Cryptolocker* (*software* malicioso), cobram cerca de US$300 para que o dono volte acessar os seus dados. Mas o dinheiro deverá ser pago dentro de 72 horas.

Uma empresa que possua uma segurança da informação/cybersecurity eficaz ganha ainda mais a confiança de seus *stakeholders* (partes interessadas), pois esses terão a certeza de que seus dados estarão protegidos, principalmente em compras realizadas pela internet. E por

isso empresas do *e-commerce* buscam cada vez mais investir em profissionais recém-formados da área de SI, fornecendo treinamentos específicos para torna-los cada vez mais capacitados, além de pagarem um bom salário, para mantê-los, pois há escassez dessa mão-de- obra.

A ISO 27001 - Gestão de Segurança da Informação é uma norma internacional que objetiva a garantia de que controles adequados estejam em vigor para que seja possível abordar os princípios da SI e proteger as informações dos stakeholders. Ajuda no desenvolvimento de um plano de continuidade do negocio, reduzindo os efeitos de um possível ataque na segurança, e a reduzir ameaças à segurança e de pontos fracos do sistema. Ao atender os requisitos da ISO 27001 demostra que a empresa atende os requisitos da Lei de Proteção de Dados de 1998. Permite parcerias com organizações que só assina contrato se essa tiver a certificação.

A gestão das empresas sempre está voltada ao gerenciamento de crises e recuperação de operações corrompidas, mas ao conhecer os princípios e mecanismos da SI é possível desenvolver uma gestão que estará focada nos limites de risco aceitáveis, através de melhores praticas da infraestrutura do negocio e de metodologias e politicas de segurança, diminuindo assim o custo com incidentes, uma vez que a empresa estará desenvolvendo mecanismos de prevenção. Com o aumento crescente dos ciberataques, é essencial que a empresa tenha um profissional capacitado para desenvolver novos mecanismos e utilizar os já existentes no âmbito da *cybersecurity*, de acordo com suas necessidades.

Portanto, as empresas devem investir em mão-de-obra qualificada e também desenvolver métodos para manter esses bons profissionais, uma vez que, um único sequestro de dados ou vazamento de informações pode custar muito caro. A melhor saída é investir em prevenção e melhoramento dos pontos fracos já existentes, utilizando alguns mecanismos e ferramentas citadas neste trabalho, além de adotar os princípios de normas certificadores como a ISO 27001, que só trará vantagens, como uma vantagem competitiva na relação de maior confiança com seus clientes.

REFERÊNCIAS

AÇÕES do Facebook caem 7% após novo vazamento. **UOL**, São Paulo, 19 dez. 2018. Disponível em: <https://economia.uol.com.br/cotacoes/noticias/redacao/2018/12/19/acoes-facebook-bolsas-eua.htm>. Acesso em: 10 de maio de 2019.

ADOBE. O que são assinaturas digitais?. Disponível em: <https://acrobat.adobe.com/br/pt/sign/capabilities/digital-signatures-faq.html>. Acesso em: 10 de maio de 2019.

ARAUJO, Nonata Silva. Segurança da Informação (TI). **Administradores.com**. Disponível em: <https://administradores.com.br/artigos/seguranca-da-informacao-ti>. Acesso em 8 de Maio de 2019.

DEMARTINI, Mariana. Hackers trancam quartos de hotel e exigem resgate em bitcoin. **Exame**. Disponível em: <https://exame.abril.com.br/tecnologia/hackers-trancam-hospedes-em-hotel-e-exigem-resgate-em-bitcoin/>. Acesso em: 10 de maio de 2019.

FELIX, Jorge Armando**.** Portaria GSIPR nº 45 de 08/09/2009. **LegisWeb**. Disponível em: <https://www.legisweb.com.br/legislacao/?id=213726>. Acesso em: 10 de maio de 2019.

JACOBSON, Roni. Sequestro de arquivos digitais: um malware chamado CryptoLocker força usuários a pagar resgate. **UOL.** 2018. Disponível em: <https://www2.uol.com.br/sciam/noticias/sequestro_de_arquivos_digitais.html>. Acesso em: 10 de maio de 2019.

LONGO, Gustavo Dobkowski. Segurança da Informação. **Ebah by Docsity.com**. Disponível em: <https://www.ebah.com.br/ >. Acesso em: 10 de maio de 2019.

MACHADO, Jonathan. O que é firewall?. **TecMundo**. Disponível em: <https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm>. Acesso em: 10 de maio de 2019.

OLIVEIRA, Déborah. 3 tendências para o mercado de segurança da informação, sendo o Gartner. **IT Forum 365**. Disponível em: <https://itforum365.com.br/3-tendencias-para-o-mercado-de-seguranca-da-informacao-sendo-o-gartner/>. Acesso em: 10 de maio de 2019.

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Karoline Galdêncio de; ARAÚJO, Francisco de Assis Noberto Galdino de. GESTÃO DA SEGURANÇA DA INFORMAÇÃO: perspectivas baseadas na tecnologia da informação (T.I.). **Revista Múltiplos Olhares em Ciência da Informação,** v.3, n.2, 2013.

ROMAGNOLO, Cesar Augusto. O que é criptografia?. **Oficina da net**. Disponível em: <https://www.oficinadanet.com.br/artigo/443/o_que_e_criptografia>. Acesso em: 10 de maio de 2019.

SILVA, Edelberto Franco; JULIO, Eduardo Pagani. Sistema de Detecção de Intrusão. **DevMedia.** Disponível em: <https://www.devmedia.com.br/sistema-de-deteccao-de-intrusao-artigo-revista-infra-magazine-1/20819>. Acesso em: 10 de maio de 2019.

VAZAMENTO de dados por empresas pode custar caro. **Folha de Londrina,** Londrina, 7 fev. 2019. Disponível em: <https://www.folhadelondrina.com.br/economia/vazamento-de-dados-por-empresas-pode-custar-caro-1026189.html>. Acesso em: 10 de maio de 2019.