**Victor Eduardo Requia, Diego Zavatini Ciências da Computação 26/08/2019**

**MAT 102 -02U Metodologia de pesquisa Adelaide Maria Bogo**

**PESQUISA BIBLIGRÁFICA**

FATO:

Recentemente, ondas de ataques cibernéticos nos quais, crackers se utilizam das vulnerabilidades para obtenção do acesso as informações de empresas e órgãos governamentais, tem sido destaque nas empresas de segurança para saber de que forma os atacantes exploraram os sistemas.

TEMA:

Problemas de proteção de informação na internet enfrentados em empresas e órgãos governamentais para proteção de suas informações.

PERGUNTA:

Quais são os principais problemas enfrentados em empresas e órgãos governamentais com relação a segurança de suas informações na internet?

Em vista das novas formas de comunicação e armazenamento, muitas empresas e órgãos públicos acabaram se adaptando às novas tecnologias e assim, otimizaram seus serviços e processos. Porém, uma questão muitas vezes desvalorizada por essas corporações é a da segurança. Com isso, vulnerabilidades nos sistemas podem acarretar em ataques maliciosos, podendo comprometer os pilares da segurança da informação, o vazamento de dados, prejuízos financeiros, roubos, deturpação das informações e até mesmo a paralização dos serviços oferecidos (PINHEIRO 2007).

Vários são os motivos que colocam em risco os sistemas. Para empresas privadas, que necessitam assegurar as informações para garantir lucros e sobrevivência do negócio (RIOS; TEIXEIRA FILHO; RIOS, 2017), a falta de incentivos econômicos é considerada um dos principais agravantes (CORTEZ; KUBOTA ,2013). Além da deficiência na escolha de sistemas mais seguros, como explica Pinheiro:

Atualmente, na quase totalidade dos casos, os sistemas de informação são escolhidos segundo as funcionalidades oferecidas e o investimento inicial, em detrimento da robustez, maturidade e do retorno do investimento a longo prazo ou benefícios indiretos (PINHEIRO, 2007 p.12).

Comitê Gestor de Informática (2009), 71,6% empresas reportaram ter encontrado algum tipo de problema relacionado a segurança da informação.

Já nos órgãos públicos, os quais devem proteger a informação, pelo direito do cidadão (RIOS; TEIXEIRA FILHO; RIOS, 2017), apesar de existir modelos para manter e melhorar a segurança como as normas ABNT da família ISO/IEC 2700 (SFREDDO; FLORES, 2012), ainda existem lacunas na parte administrativa das corporações para a adesão ou a prática destas (GUIMARÃES; SOUZA NETO; LYRA, 2018). Como ocorre, nas instituições federais de ensino superior, cada polo tem suas regras de conduta sendo responsável pela segurança da informação e comunicação. Assim, muitas acabam deixando algumas questões de lado Rios et al (2017), 51% das instituições adotaram totalmente a política de segurança da informação e 15%, parcialmente.

Ou seja, 34% das instituições pesquisadas não possuíam uma Política de Segurança da informação e Comunicação – PoSIC. Ademais, com a normatização e obrigatoriedade da divulgação de dados e informações de interesses públicos como na Leis de Acesso à Informação, para garantir a publicidade, aumentou imensamente o número de dados expostos na rede. Apesar de beneficiar o cidadão, muitas vezes o tratamento de dados não segue um padrão e muitas informações confidencias como a de agentes públicos, são expostas (SANCHES et al 2016).

Além dos problemas citados, que diferem das esferas públicas e privadas, existe um problema geral. O despreparo ou a má conduta de quem opera o sistema (WORKMAN; BOMMER; STRAUB, 2008). Para Furnell e Thomson (2009), um dos problemas mais comuns na segurança da informação é o comportamento e ação dos funcionários, que por vezes são vistos como obstáculos da segurança.

Por isso, é importante moldar as crenças, valores, habilidades e mentalidade de quem trabalha na mesma. Segundo o Comitê Gestor de Informática (2009), ao analisar empresas que sofreram ataques cibernéticos, houve uma relação positiva entre o número de funcionários que obtinham acesso a rede de internet com os problemas de segurança.Por isso, o treinamento é essencial para as corporações, principalmente para evitar ataques já conhecidos e usualmente relatados como é o caso da engenharia social, no qual o atacante se utiliza da confiança e manipulação do contratado como meio para fraudar ou adquirir informações restritas (COELHO; RASMA; MORALES; 2013).

Fernandes e Souza (2016), 45 servidores públicos, mostraram que o despreparo e erros cometidos são elevados. Cerca de 60% dos entrevistados precisavam enviar informações sigilosas por e-mail, 69% permitiram o acesso remoto do computador e mais da metade não estava ciente de quem o acessava, além do mais, 47% confia muito ou totalmente em outros.

Com o que foi exposto, observa-se que tanto no setor público como privado, a segurança com a informação ainda é duvidosa. E as principais causas que levam aos problemas citados durante a pesquisa são a falta de interesse, tratamento inadequado dos dados e motivos financeiros na administração pública e privada respectivamente.

REFERÊNCIAS

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. engenharia social: uma ameaça à sociedade da informação. **Exatas & Engenharia**: Perspectivas OnLine, [s.i], v. 3, n. 5, p.34-44, 23 mar. 2013.

COMITÊ GESTOR DE INFORMÁTICA. **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil:** TIC Domicílios e TIC Empresas 2009. São Paulo. 2010. Disponível em <www.cetic.br/media/analises/tic-empresas-2009.pdf>. Acesso em 01 set. 2019.

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas de segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista de Administração**, [s.l.], v. 48, n. 4, p.757-769, 19 dez. 2013. Business Department, School of Economics, Business & Accounting USP.

FURNELL, Steven; THOMSON, Kerry-lynn. From culture to disobedience: Recognising the varying user acceptance of IT security. **Computer Fraud & Security**, [s.l.], v. 2009, n. 2, p.5-10, fev. 2009. Elsevier BV.

GUIMARÃES, Rogério; SOUZA NETO, João; LYRA, Mauricio da Rocha. Modelo de governança de segurança da informação para a administração pública federal. **Perspectivas em Gestão & Conhecimento**, João Pessoa, v. 3, n. 8, p.90-109, 26 dez. 2018.

RIOS, Orlivaldo Kléber Lima; TEIXEIRA FILHO, José Gilson de Almeida; RIOS, Vânia Patrícia da Silva. Gestão de segurança da informação: práticas utilizadas pelas instituições federais de ensino superior para implantação de política de segurança da informação. **Navus - Revista de Gestão e Tecnologia**, [s.l.], p.49-65, 10 abr. 2017. Servico Nacional de Aprendizagem Comercial.

PINHEIRO, José Maurício dos Santos. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. **Cadernos Unifoa**, [s.i], v. 3, n. 5, p.11-21, 5 dez. 2007.

SFREDDO, Josiane Ayres; FLORES, Daniel. Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. **Perspectivas em Ciência da Informação**, [s.l.], v. 17, n. 2, p.158-178, jun. 2012.

SOUZA, Raul Carvalho; FERNANDES, Jorge Henrique Cabral .Um estudo sobre a confiança em segurança da informação focado na prevenção a ataques de engenharia social nas comunicações digitais. **Brazilian Journal of Information Science: research trends**, [S.I], v. 10, n. 1, p.63-75, 1 mar. 2016.

WORKMAN, Michael; BOMMER, William H.; STRAUB, Detmar. Security lapses and the omission of information security measures: A threat control model and empirical test. **Computers In Human Behavior**, [s.l.], v. 24, n. 6, p.2799-2816, set. 2008. Elsevier BV.