UMA ANÁLISE SOBRE NOÇÕES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE DO IFSULDEMINAS

Thales A. REIS[1];Emerson A. de CARVALHO[2]

RESUMO

A informática vem mudando os hábitos das pessoas mundo a fora. No Brasil não é diferente, com uma estimativa de termos um dispositivo computacional para cada habitante em dois anos (até 2017). O acesso à Internet também cresce a uma velocidade considerável (40% entre 2009 e 2011). No entanto, a segurança no uso dos dispositivos computacionais, em especial aos conectados em rede, não é tratada com a devida atenção que merece. Segundo um relatório da Organização das Nações Unidas (ONU), em sua Conferência sobre Comércio e Desenvolvimento (Unctad), o Brasil é um dos cinco países com mais crimes cibernéticos. Considerando a relevância do tema, este artigo visa caracterizar a comunidade do IFSULDEMINAS no que diz respeito às noções sobre Segurança da Informação e aos principais fatores de riscos aos quais estão sujeitos ao desempenhar suas atividades diárias que envolvem o uso de dispositivos computacionais em rede.

Palavras-chave:

Segurança da Informação; Cibersecurity; Hackers; Segurança Computacional; Segurança Digital.

1. INTRODUÇÃO

O bem durável que mais cresce nos lares brasileiros é o computador (crescimento de quase 40% entre 2009 e 2011, com aproximadamente 79,9 milhões de brasileiros) (IBGE, 2011). O acesso à *Internet* também cresce rapidamente. Aproximadamente 65% dos domicílios brasileiros possuem dispositivos computacionais (computadores pessoais, *laptops* e *tablets*), o que significa aproximadamente 40 milhões de lares (CETIC.br, 2013).

O CERT (CERT.br, 2014), no ano de 2013, registrou um total de 352.925 incidentes de segurança no Brasil. Desse total, 85.675 foram tentativas de fraude, que se caracteriza por um ato enganoso, de má-fé, com intuito de lesar ou ludibriar alguém. A Central Nacional de Denúncias de Crimes Cibernéticos (CNDCC), mantida pela SarferNet (SAFERNET, 2014), recebe diariamente uma média de 2.500 denúncias envolvendo crimes de pornografia infantil ou pedofilia, racismo, neonazismo, intolerância religiosa, apologia e incitação a crimes contra a vida, homofobia e maus tratos contra os animais.

[1] Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Passos. Passos/MG. E-mail: thalesreis57@gmail.com

[2] Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – Campus Machado. Machado/MG - E-mail: emerson.carvalho@ifsuldeminas.edu.br

Um conceito importante relacionado à Segurança da Informação é de que não existe segurança absoluta. Ao invés de perseguir uma garantia absoluta na segurança, é mais importante conscientizar as pessoas para que tenham atitudes seguras (MARÇULA; FILHO, 2013). A educação é uma maneira econômica de empresas e instituições de ensino alcançar uma segurança mínima. Este trabalho visa caracterizar a comunidade do IFSULDEMINAS no que diz respeito às noções sobre Segurança da Informação e aos principais fatores de riscos aos quais discentes, docentes e demais servidores estão sujeitos ao desempenhar suas atividades diárias que envolvem o uso de dispositivos computacionais em rede.

2. MATERIAL E MÉTODOS

O trabalho fundamentou-se numa pesquisa aplicada, objetivando gerar conhecimentos para tomada de ações relacionadas ao uso seguro de dispositivos computacionais. Foi desenvolvida sobre uma abordagem não experimental, e sim por um levantamento realizado por questionários on-line para sua elaboração e execução. Discentes, Docentes e TAEs de diversos cursos e campi do IFSULDEMINAS formaram a amostra. Baseado nos índices de ataques reportados ao CERT.br e CNDCC, foram selecionados ataques e vulnerabilidades de maior risco, considerando o público alvo da pesquisa (não profissionais em informática), para comporem o conteúdo da pesquisa.

O questionário considerou situações do cotidiano das pessoas durante as atividades que envolvam dispositivos computacionais, de forma que os riscos inerentes pudessem ser avaliados naturalmente. O objetivo foi verificar se as pessoas saberiam identificar situações de risco que nos são apresentadas a todo momento, tais como: fraudes de antecipação de recursos, rastreamento de atividades, falsificações de e-mails, furtos de identidade, *Cyberbulling*, códigos maliciosos (vírus, *worm*, cavalo de tróia etc), criação de senhas seguras, *sexting*, uso de criptografia (https) etc.

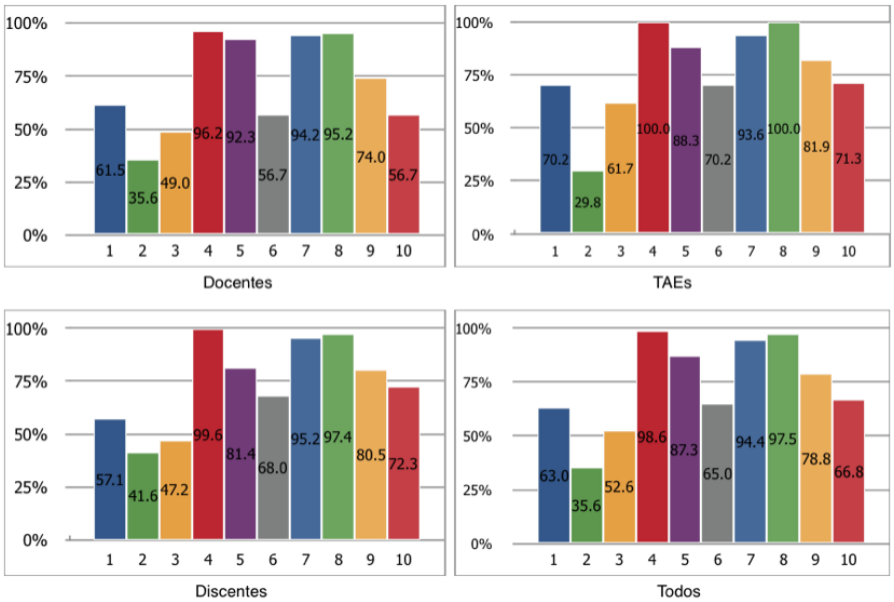
3. RESULTADOS E DISCUSSÕES

A Figura 1 mostra o percentual de acerto (vertical) em relação às vulnerabilidades analisadas (horizontal). Analisamos os resultados com base nas vulnerabilidades, separadas em três grupos. Aquelas cujo nível de acerto médio (considerando todo o público) foram superior a 80% (grupo A), aquelas cujo nível médio foi inferior a 80%, porém superior a 60%

(grupo B) e aquelas cujo nível médio foi inferior a 60% (grupo C). Classificamos dessa forma por entender que essa escala pode ser usada para priorizar ações de conscientização em relação a cada grupo de vulnerabilidades, não temos o objetivo de determinar que, por ser ou não mais conhecido, uma determinada vulnerabilidade representa maior ou menor risco. O grupo A é composto por quatro vulnerabilidades: Furto de identidade, Spam, Códigos maliciosos e *Cyberbulling*. O grupo B por quatro vulnerabilidades: *Cookies*, Senhas seguras, Criptografia https e *Sexting* e privacidade e o grupo 3 é composto por duas vulnerabilidades: Falsificação de e-mail e Fraude de antecipação de recurso. É observado que há um bom entendimento em relação às vulnerabilidades do grupo A, o que mostra um público menos exposto aos riscos causados por antigas e tradicionais vulnerabilidades, como *Spans*, vírus, falsificações ideológicas e *Cyberbulling*. O entendimento do público em relação às vulnerabilidades do grupo B não se mostra satisfatório, isso se dá ao verificarmos que aproximadamente 35% do público não reconhecem as práticas recomendadas para se criar uma senha segura, 33% não reconhecem a relação da prática de *Sexting* com a possível violação de sua privacidade e 37% não reconhecem a relação do rastreamento das suas atividades online às *Cookies*, além de 21% não reconhecerem a relação do protocolo https à criptografia dos dados trafegados. Os resultados relacionados ao grupo 3 são preocupantes, pois 64% do público não reconheceram uma situação onde poderia haver uma falsificação de e-mail e 47% não se mostraram atentos a uma possível fraude de antecipação de recursos. No geral, independente da vulnerabilidade e do perfil do público, 26% das situações de risco não foram corretamente reconhecidas. De fato, reconhecer corretamente o risco não seria um problema, o problema maior é quando não há a consciência de que há um risco iminente.

4. CONCLUSÕES

Nosso principal objetivo foi analisar o entendimento dos diversos riscos para poder subsidiar o planejamento e criação de recursos que tornem a vida online menos perigosa. Os resultados obtidos nos mostra que há uma uniformidade em relação aos riscos no que diz respeito ao público analisado. Isso nos leva à necessidade de elaborar ferramentas (treinamentos, palestras, materiais impressos etc) que esclareçam nossa comunidade em relação às vulnerabilidades cujo entendimento foi menor que o esperado (grupos 2 e 3).



1) Cookies; **2)** Falsificação de email; **3)** Antecipação de recursos; **4)** Furto de identidade; **5)** Spam; **6)** Senhas seguras; **7)** Códigos maliciosos; **8)** Cyberbulling; **9)** Criptografia (https); **10)** Sexting e privacidade

Figura 1: gráfico de acertos para cada público e vulnerabilidade

É clara a necessidade de ações que aumentem o entendimento e a capacidade das pessoas em lidar com situações de riscos, como: senhas fracas, a troca de informações intimas, falta de conhecimento das ferramentas, protocolos e ambientes (como e-mail). Em um ambiente onde a educação é o objetivo maior, é necessário educar, constantemente, educadores e educandos em relação ao uso mais consciente das ferramentas tecnológicas.

5. REFERÊNCIAS

IBGE. PNAD - Pesquisa Nacional por Amostra de Domicílios, 2011.

CETIC.br 2013 CETIC.br. Pesquisa sobre o uso das tecnologias de informação e comunicação no brasil-tic domicílios. Disponivel em <http://cetic.br/pesquisa/domicilios/indicadores>. Acessado em 21 de abr. 2015.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em < http://www.cert.br/>. Acesso em: 01 dez. 2014.

SAFERNET. SAFERNET BRASIL. Disponível em: <http://www.safernet.org.br/>. Acesso em: 03 dez. 2014.

MARÇULA, M.; FILHO, P. A. B. INFORMÁTICA - CONCEITOS E APLICAÇÕES. 4ª ed. São Paulo, Érica, 2013.