A IMPORTÂNCIA DA SI PARA O INSTITUTO FEDERAL DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO.

Daniel Alves da Silva (1); Airton Santiago (2); Thiago Hildefonso Nogueira (3); Severino do Ramo de Paiva (4)

1Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta, danielws38@hotmail.com
2Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta, santiagoass2016@gmail.com
3Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta, thiagohildefonso378@gmail.com
4Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano – Campus Floresta, severino.paiva@ifsertao-pe.edu.br

Resumo: Este trabalho tem como foco a análise no que diz respeito a segurança da informação no Instituto Federal de Educação Ciência e Tecnologia do Sertão Pernambucano, dando ênfase a gestão de SI dessa empresa pública. Baseando-se em recentes e históricos de ataques e trabalhando com as informações e dados a respeito, o artigo visa mostrar vulnerabilidades, ameaças e ataques recorrentes na instituição, Usando de metodologia de caráter exploratório, foram procurados documentos para conceituar os principais métodos de ataques e o que pode ser feito para evitá-los sabendo-se que os dados e informações de funcionários e alunos são de extrema importância no setor de ensino mostrando a importância da SI neste setor. Será destacado desde o conceito da Segurança da Informação (SI), a sua necessidade para as instituições de ensino bem como o estudo de vulnerabilidades, ameaças e ataques. Foi dado o conceito dos quatro princípios básicos de Segurança da Informação (SI) que é a confiabilidade, integridade, disponibilidade e autenticidade, desobedecendo qualquer um desses princípios pode causar grandes prejuízos para as instituições de ensino e organizações. Foi estudado a política de segurança da informação e serviços oferecidos pelo site da instituição. Foi utilizado o estudo de caso para identificar quais os ativos precisavam ser protegidos e também foi feita uma análise de risco, para identificar os riscos mais altos, com objetivo de tratá-los e preveni-los das ameaças encontradas. Por fim foram apresentados o catálogo de serviços do site da instituição, dando ênfase ao SAGE, como um dos principais serviços, e outros ataques registrados, além de possíveis trabalhos futuros mostrando enfim, a importância da segurança da informação para a rede de ensino.

Palavras-chave: Segurança da Informação. Educação. Ataques, Instituição.

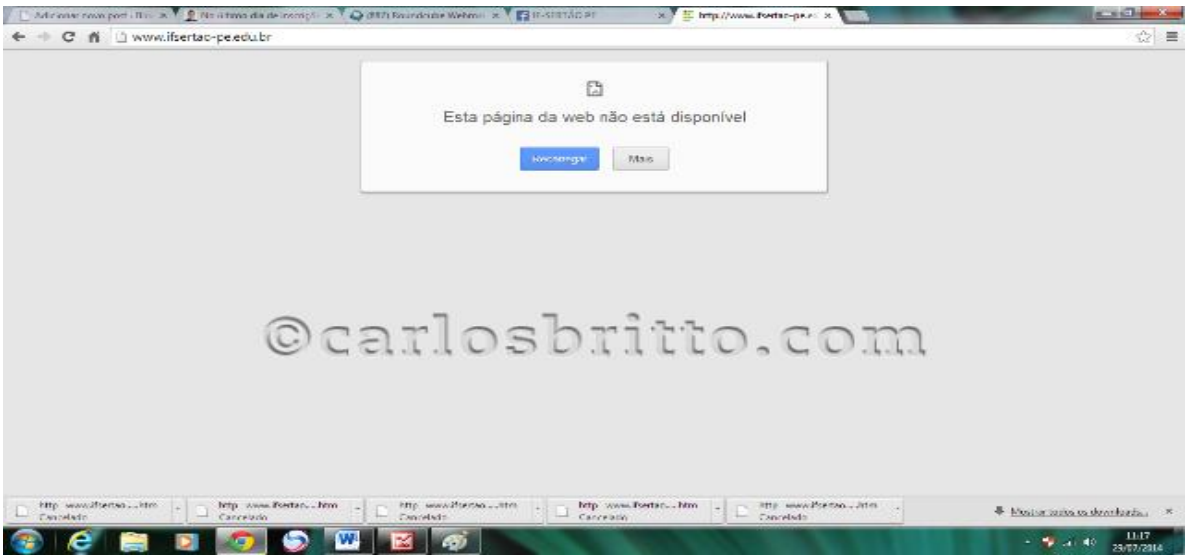
1. INTRODUÇÃO

Nos últimos anos, as empresas públicas e privadas têm se preocupado em investir na proteção de suas informações e dados pessoais tendo em vista que a evolução recente da internet e a grande quantidade de usuários que a utilizam geram vulnerabilidades e ameaças para essas instituições.

Como exemplo de instituição federal de ensino, o Instituto Federal de Educação Ciência e tecnologia do Sertão Pernambucano (IF-Sertão) tem sofrido ataques de violando o princípio da disponibilidade da Segurança da Informação (SI). As vulnerabilidades da instituição tem sido um canal para os invasores, o ataque principal tem sido a negação de serviço (Denial of Service), que por sua vez vem prejudicando servidores e alunos que necessitam de suas informações disponíveis.

A segurança da informação é de extrema importância para o setor ensino, principalmente se tratando de dados e informações dentro de uma instituição acadêmica. A confiabilidade, integridade, disponibilidade e autenticidade são princípios básicos que compõem a SI para manter a segurança dentro de qualquer organização. No entanto, com a quebra desses pilares a informação se torna vulnerável comprometendo o seu sigilo.

Figura 1 - Site do IF-Sertão fora do ar



Fonte: http://www.carlosbritto.com/wp-content/uploads/2014/07/Sem-t%C3%ADtulo2.png.

A imagem acima mostra o ataque de negação de serviço (Denial of Service), ao site do IF-Sertão deixando o site fora do ar, impossibilitando servidores e alunos a acessarem suas informações. O incidente acontecido violou um dos quatro princípios básicos de segurança da informação, o princípio da disponibilidade que garante o acesso das informações sempre que necessário.

Baseado nisso, este trabalho científico tem como objetivo geral:

- Investigar históricos de ataques, ameaças, e vulnerabilidades no IF-Sertão, ajudando na proteção dos ativos do IF-Sertão.

E específicos:

- Analisar os serviços oferecidos pelo site da instituição.
- Investigar a estrutura e política de segurança do IF-Sertão.
- Explorar ataques já ocorridos na instituição.

2 REVISÃO BIBLIOGRÁFICA

Apesar da segurança ser, atualmente, essencial para os negócios das organizações, a dificuldade em entender sua importância ainda é muito grande. Muitas vezes, a única segurança existente é a obscuridade. (NAKAMURA; GEUS, 2007, p 51 apud PAIVA, Severino do Ramo de; Segurança e Auditoria de sistemas, 2017, p 24).

2.1 O que é segurança da informação.

A segurança da informação protege ativos de uma organização, contra problemas acidentais ou propositais, além minimizar os riscos e impactos destes possíveis incidentes.

2.2 Princípios da SI.

Figura 2 - Pilares da SI

Fonte: http://periciacomputacional.com/wp-content/uploads/2017/01/cia1.jpg

A segurança da informação tem como base esses quatros princípios citados na figura 2 que visa manter proteção das informações preservando o valor que possui para o proprietário ou para uma organização.

O princípio da confidencialidade, visa garantir que as informações ou dados armazenados esteja acessível apenas para pessoas autorizadas.

O princípio da integridade, visa garantir que as informações enviadas não sejam violadas indevidamente, mas que mantenha as características originais estabelecidas pelo proprietário da informação.

O princípio da disponibilidade, visa garantir que a informação estará sempre acessível para o usuário sempre que lhe for necessário.

O princípio da autenticidade, visa garantir a identidade do proprietário ou empresa que manipula suas informações.

2.3 O que são ataques, vulnerabilidades e ameaças.

“De acordo com a NBR ISO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças” (PAIVA, 2017, p. 66). As vulnerabilidades são brechas localizadas em equipamentos, softwares, recursos humanos e políticas dentro da organização. Essas falhas por si só não causam danos a organização, pois necessita de um agente causador.

Códigos maliciosos, também conhecidos como pragas e malware, programas desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos, como computadores, modems switches, roteadores e dispositivos móveis (tablets, celulares, smartphones, etc.) CERT.br (2017,Pag.02) apud PAIVA, Severino do ramo de - Segurança e auditoria de sistemas (2017, Pag.55).

De acordo com a citação acima as ameaças são códigos maliciosos que são capazes de infectar programas computacionais e usurpar informações confidenciais. Segundo (PAIVA, 2017, p. 66) “as ameaças que são utilizadas para realização de ataques, estes com o objetivo de modificar ou captar informações de ativos, ou informações intangíveis de informática, como, software, ou programas de banco de dados, ou informações, ou ainda a imagem corporativa ”. Esse evento pode acarretar incidentes indesejados para organização resultando em prejuízos.

2.4 SI no âmbito educacional:

Segundo o site Canaltech, as instituições educacionais como escolas, colégios e universidades também são alvos frequentes de ameaças que podem causar grandes danos às redes corporativas, além então do roubo de informações confidenciais e ataques à imagem dessas empresas. O mesmo ainda relata que é muito importante que a estrutura de TI da instituição educacional seja dividida em redes isoladas, que a estrutura seja adaptada para o negócio e que a segurança seja pensada ativamente. A manutenção tem que ser intensa e contínua, o ambiente acadêmico deve ser separado do administrativo, mas ambos precisam de muito investimento em segurança incluindo a relação de eventos genéricos, monitoramento, firewall, antivírus, entre outras soluções.

3 METODOLOGIA

Método de coleta de dados:

A pesquisa será de caráter exploratório, levando em conta fatos, acontecimentos históricos, registro de ataques e precauções referentes a Segurança da Informação no IF-Sertão, estudo de sua política de segurança da informação e serviços oferecidos pelo site, e baseando-se na análise de vulnerabilidades, ameaças e ataques aos ativos desta empresa pública.

Método de Análise de dados:

Todos os dados serão documentados de maneira que as informações referentes a situações serão avaliadas qualitativamente, e os relatos da quantidade de determinados parâmetros será analisado quantitativamente.

4 RESULTADOS E DISCUSSÕES

Figura 3 – Catalogo de Serviços do site do IF-Sertão

Fonte: http://www.ifsertao-pe.edu.br/dgti/servicos/

A figura 3, mostra parte do catálogo de serviços do IF-Sertão que devem ser protegidos:

- Acadêcimos: SAGE, SAGE PRONATEC, Biblioteca, SRSC, Manual do Usuário, PIT/RIT, SistEX, Certificados, Validar Certificado, CAFe, SRD, SisuSAGE, SPSSAGE, SCPP, SCE.

- Administrativo: SUAP, Solicitar E-mail, Diárias e Passagens, Relatórios, Gestão de Projetos, SiCABS, Remoção Interna, Manuais, VideoAulas,Webconferência.

- Gerais: Site Institucional: Colabore, Agenda, Processo Seletivo, Concursos Públicos.

Figura 4 – Sistema SAGE.

Fonte: https://sage.floresta.ifsertao-pe.edu.br/

A imagem mostra o Sistema de Apoio à Gestão Educacional (SAGE), um dos mais importantes serviços que está vinculado ao site do IF Sertão. O SAGE é uma ferramenta utilizada por alunos e servidores do IF-Sertão para ter acesso às suas informações de maneira detalhada. Foi desenvolvido pela equipe de Tecnologia da Informação do IF.

Observa-se a falta de segurança quando os alunos tentam ter acesso às suas informações no SAGE, pois a ferramenta utiliza o número da matrícula como login e também utiliza como senha. Isso acarreta falta de segurança para o usuário, pois se um indivíduo tem acesso ao número da matrícula de outra pessoa ele facilmente pode modificar os dados do usuário. Este ato faz com que o atacante desobedeça um dos quatro princípios da SI, o da Integridade, pois o atacante modificou os dados de outra pessoa sem autorização.

Sobre a política de segurança da informação da instituição, a mesma é composta pela resolução nº. 13 do conselho superior, de 22 de junho de 2016. Elaborado pelo comitê gestor de segurança da informação, possui aspectos de princípios, gestão de riscos, incidentes, até penalidades.

Trabalhos futuros:

O site do IF-Sertão possui links de sites da equipe especializada em segurança e TI da instituição. Estão sendo efetuadas buscas nesta área. A mídia não possui dados a respeito de relatos de ataque, porém, estão sendo procuradas novas formas de aquisição de conteúdo, sejam dados ou informações, bem como os mesmos estão sendo encontrados e serão brevemente analisados. Além da possibilidade do uso da ferramenta Nmap para testar na prática o como se sai a segurança do sistema web.

5 CONCLUSÕES

Neste trabalho foi apresentado um estudo analítico sobre segurança da informação no Instituto Federal de Educação Ciência e Tecnologia do Sertão Pernambucano, tendo como foco a proteção de ativos informacionais dessa organização, abordando sua cultura organizacional, que é um fator crucial para implementação de uma política de segurança da informação. O estudo de caso identificou ativos que precisam ser protegidos, sendo eles os serviços do site da instituição. Realizou-se também uma pesquisa sobre a Política de Segurança da Informação da instituição, mostrando que a SI é um fator crítico e deve ser levado em conta na gestão de projetos e no plano estratégico de uma organização, também como uma forma de obtenção na qualidade dos negócios.

6 REFERÊNCIAS

RIOS, Orlivaldo Kleber Lima. TEIXEIRA FILHO, José Gilson 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.** Disponível em: http://navus.sc.senac.br/index.php/navus/article/download/482/pdf Acesso em 18.09.2017.

CASTILHO, Sergio Duque; FONTE, Miguel Feitosa da: **Política de segurança da informação aplicada em uma instituição de ensino mediante análise de risco**. Disponível em: http://retec.fatecourinhos.edu.br/index.php/retec/article/view/99/144 Acesso em: 18.09.2017

PAULA, Lorena Pires de; CORDEIRO, Douglas Farias: **Políticas de segurança da informação em instituições públicas**. Disponível em: http://periodicos.unifacef.com.br/index.php/resiget/article/download/1046/843 Acesso: 08/10/2017.

PINHEIRO, José Maurício dos Santos: **Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar.** Disponível em: http://web.unifoa.edu.br/cadernos/edicao/05/11.pdf Acesso: 08/10/2017.

Canaltech: **O gerenciamento da segurança da informação em escolas e universidades**. Disponível em: https://canaltech.com.br/seguranca/O-gerenciamento-da-seguranca-da-informacao-em-escolas-e-universidades/ Acesso: 08/10/2017.

PAIVA, Severino do Ramo de: **Segurança e Auditoria de Sistemas**. IMPRELL, 2017.

IF-Sertão, **POLITICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (POSIC).** Disponível em: https://www.ifsertao-pe.edu.br/images/Reitoria/Dgti/.../posic_2006_resolucao_13.pdf Acesso em: 16/10/2017.