PROJETO DE PESQUISA

Análise de vulnerabilidades com foco na segurança da informação aplicada à ambiente de ensino superior

Prof. Me. Guilherme Lopes Matsushita (Orientador) – Mestre em Tecnologia da Inteligência pela PUCSP – Faculdade Anhanguera de Guarulhos

Cauê Nunes da Silva – Graduando em Tecnologia em Análise e Desenvolvimento de Sistemas – Faculdade Anhanguera de Guarulhos

FACULDADE ANHANGUERA DE GUARULHOS

Guarulhos / SP

2019

Análise de vulnerabilidades com foco na segurança da informação aplicada à ambiente de ensino superior

RESUMO

O presente trabalho visa apresentar um relato sobre o projeto de pesquisa em andamento, que analisa todas as vulnerabilidades, ameaças e riscos contra um ambiente de ensino superior, em sua estrutura física e lógica, relacionadas à segurança da informação. Este trabalho tem como objetivo apresentar as dificuldades em elaborar um relatório de segurança da informação, contendo todas as situações que expõe os usuários em risco com seus dados, seus dispositivos e também as informações corporativas e os recursos tecnológicos. O estudo de caso em andamento está sendo realizado no campus da Faculdade Anhanguera de Guarulhos, com o acompanhamento do professor Guilherme Matsushita e os alunos do curso de Tecnologia em Análise e Desenvolvimento de Sistemas. Como resultado, serão apresentados os levantamentos iniciais do projeto e seus respectivos direcionamentos.

Palavras-chave: vulnerabilidade; riscos; segurança; ensino superior.

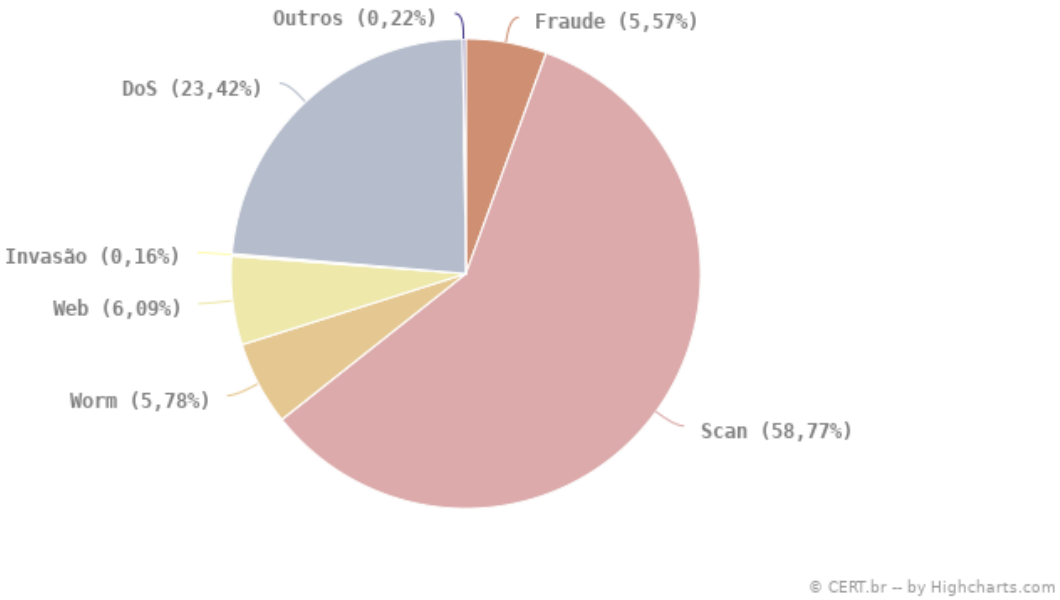
INTRODUÇÃO

A segurança da informação é um tema sempre atual no cenário da tecnologia da informação, direcionado às empresas de qualquer segmento como um todo, de acordo com LOBO (2019, p.15). Lidar com a insegurança é correr riscos desnecessários, colocando o patrimônio sob ameaças físicas e digitais. No mundo contemporâneo que vivemos, na era da informação digital, os ataques estão cada vez mais presentes e tornando o ambiente empresarial em uma espécie de bolha protegida, porém com algumas aberturas que devemos nos atentar ou as vezes não sabemos dessas brechas.

A análise de risco, conforme descrita por FERREIRA (2003, p.94) se refere ao levantamento de vulnerabilidades que o ambiente por propor tanto para os usuários quanto para a empresa, considerando os recursos tecnológicos, os ativos e a estrutura física como um todo. Essa análise deve observar as ameaças físicas e lógicas, toda e qualquer situação de risco que possa colocar os dados e as informações da empresa, disponíveis para pessoas não autorizadas ou mal-intencionadas com o objetivo de destruir dados ou roubar informações privilegiadas.

Os ataques do tipo “scan[1]” são mais comuns do que possamos imaginar, de acordo com as estatísticas apuradas pela CERT.br, o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT, 2018), conforme a figura 1. Esse tipo de ataque identifica um computador ativo conectado à Internet e quais os serviços disponibilizados podem ser utilizados como porta de entrada para o ataque ser bem sucedido.

Figura 1 – Incidentes reportados ao CERT.br de janeiro a dezembro de 2018



Fonte: https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html

OBJETIVOS

O objetivo do presente projeto de pesquisa é apresentar o estudo realizado como varredura no ambiente do ensino superior, apontando as vulnerabilidades físicas e lógicas com foco na segurança da informação, diagnosticando os riscos e oferecendo a solução mais adequada para a proteção e prevenção contra ataques ou acessos indevidos.

METODOLOGIA

O projeto de pesquisa está sendo desenvolvido de acordo com as metodologias de levantamento de informações, tanto do tipo qualitativa quanto quantitativa (COSTA, 2015), pois é necessário estimar o número de pessoas (usuários, estudantes, colaboradores, fornecedores, entre outros) envolvidas no processo de utilização dos recursos, ferramentas e equipamentos tecnológicos da empresa. Esse levantamento inicial foi planejado como uma

[1] Scan - notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

análise superficial das possibilidades de ataques físicos ao prédio da organização educacional. A diante, uma nova varredura, do tipo lógica, será implementada na rede corporativa (rede local) para averiguação das configurações de segurança, ferramentas contra ataques e *softwares* antivírus ou *firewalls*.

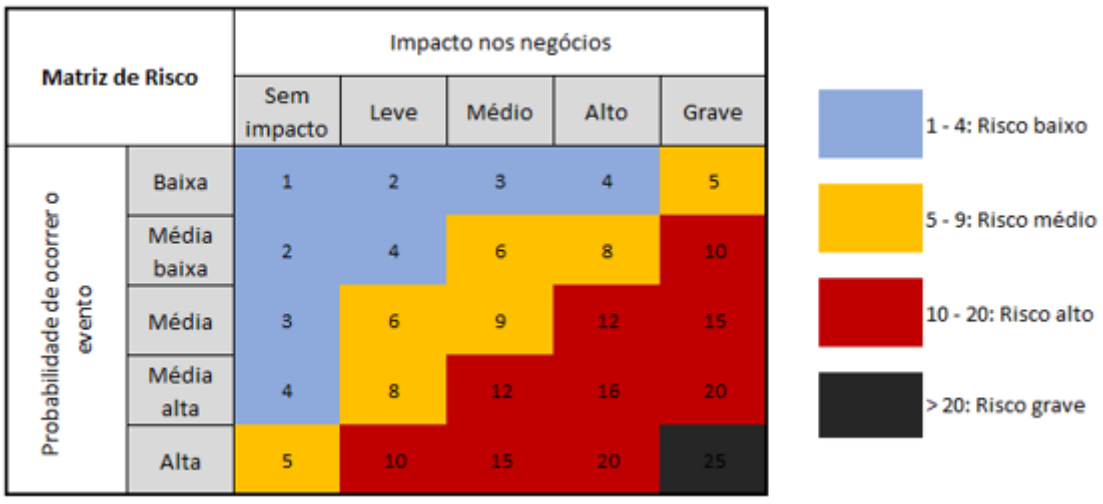
DESENVOLVIMENTO

A análise das vulnerabilidades sobre a segurança da informação no ambiente educacional da Faculdade Anhanguera de Guarulhos – Campus Pio XII, inicia com uma varredura superficial em todo o prédio, buscando apontar falhas físicas que colocam em ameaça os dados e informações da organização, os equipamentos e recursos disponíveis e também a segurança e integridade das pessoas que frequentam ou utilizam o prédio da faculdade.

O projeto conta com a participação dos alunos do terceiro semestre do curso de Tecnologia em Análise e Desenvolvimento de Sistemas, para realizar o levantamento e identificação das falhas apresentadas, gerando um relatório sobre os problemas com recursos ou falta de soluções para combater ou reduzir ações de pessoas não autorizadas ou mal-intencionadas.

A definição da situação atual em relação à exposição aos riscos foi dada, com base no cruzamento de dois fatores, a probabilidade de um evento negativo ocorrer e danificar ou prejudicar os recursos ligados aos dados, com o impacto gerado aos negócios caso ocorra tal evento inesperado. Para isso foi utilizado uma matriz de riscos elaborada em sala de aula, conforme figura abaixo.

Figura 2 – Matriz de riscos da Faculdade Anhanguera de Guarulhos



Fonte: elaborada pelo autor

Outro ponto importante é o levantamento lógico relacionado à infraestrutura de tecnologia de rede, servidores, computadores e dispositivos da rede local e rede Wi-Fi[2]. Através de entrevistas e questionários aplicados às pessoas responsáveis pela área de tecnologia e infraestrutura, e também aos colaboradores de alguns departamentos estratégicos administrativos, houve uma colaboração a fim de identificar pontos a serem analisados com maior detalhamento, para averiguar a possibilidade de ameaça real de ataque ou exploração do domínio ou dos sistemas internos.

Fato é que, por conta de permissões prévias ao responsável de tecnologia do grupo Kroton, foi feita uma análise básica e superficial em toda a rede, verificando pontos de nível de risco ou ameaça à ataques, ferramentas utilizadas e recursos de proteção, bloqueio e monitoramento do uso de sistemas e da navegação a Internet.

Resultados parciais

Inicialmente, foi diagnosticado alguns pontos a serem considerados de nível baixo de segurança, como a identificação e entrada de pessoas não autorizadas ao espaço interno do prédio principal. É necessário mudar o processo de identificação das pessoas (alunos ou colaboradores) pois de acordo com o horário, existem momentos em que a entrada fica desguarnecida de segurança para a devida identificação.

Foi instalado o sistema de catracas eletrônicas com a utilização de leitores de cartão com chip de identificação do aluno ou do colaborador, porém o sistema que faz a validação é precário em seu processamento, o que atrasa a entrada e dificulta a passagem de pessoas devidamente autorizadas.

Outro ponto crucial para o projeto, foi a verificação do uso da rede sem fio (Wi-Fi) da faculdade. O fato de a internet ser compartilhada em todo o ambiente interno da unidade, requer atenção ao uso e acesso por parte dos usuários, pois a rede não possui configuração de criptografia, nível médio de segurança para navegação e o tipo de proteção WPA com a utilização de usuário e senha de fácil acesso ou combinação.

A busca por situações de ameaça contra a informação digital da empresa, deve ser tratada com alto rigor, pois pode colocar em risco os negócios da organização, ou ter dados roubados em troca de pagamentos, como no caso de ataques do tipo r*ansonware*.

[2] **Wi-Fi** é uma abreviação de “Wireless Fidelity”, que significa fidelidade sem fio, em português. Wi-fi, ou wireless é uma tecnologia de comunicação que não faz uso de cabos, e geralmente é transmitida através de frequências de rádio, infravermelhos, etc.

Portanto, é sempre importante salientar a periódica vistoria e monitoramento do ambiente corporativo, para identificar novas possibilidades de fragilidades, do tipo física e do tipo lógica. Essas aberturas devem ser analisadas, para entender seus processos, utilizações e motivos de aplicação para definir quais serão as melhores medidas, descritas por FERNANDES (2014, p.56) a serem tomadas em relação a segurança da informação.

CONSIDERAÇÕES FINAIS

O levantamento no ambiente educacional da Faculdade Anhanguera de Guarulhos foi determinante, do ponto de vista acadêmico, pois apresentou aos alunos o universo de possibilidades de atuação profissional que o estudante formado em Sistemas da Informação ou Tecnologia em Análise e Desenvolvimento de Sistemas pode aplicar na sua carreira.

Outro fato importante a destacar é o acompanhamento do professor, com a disciplina de segurança da informação, pois proporciona uma vivência melhor do que é ensinado na teoria e visto em sala de aula.

Trabalhos futuros

Este trabalho de pesquisa, está em andamento, pois foi realizado somente uma parte de um planejamento de execuções em torno da segurança física e lógica, determinando suas vulnerabilidades e condições atuais de uso e proteção dos dados e informações digitais.

O próximo passo será uma varredura nos sistemas de gerenciamento de rede, em busca de configurações frágeis. Essa análise, deve apontar situações de risco para os usuários, e também ao gerenciamento de dados e arquivos internos.

Sendo assim, o trabalho deve relatar como uma empresa do ramo educacional pode oferecer melhores condições de segurança da informação para seus usuários, no que tange o uso da sua rede interna, a conexão com a internet via sem fio, e também todo o arquivamento de dados de uso interno e externo por parte dos colaboradores.

A Faculdade Anhanguera de Guarulhos participa e colabora para um ambiente mais seguro com o uso de políticas de segurança, metodologias e procedimentos que são adotados por todos, para que a continuidade dos negócios seja estabelecida e protegida em qualquer situação de risco ou vulnerável as ameaças digitais, naturais, sociais, humanas ou tecnológicas.

A segurança da informação, do ponto de vista dos riscos é um assunto de total importância não somente para as instituições educacionais, e sim para organizações que queiram estabelecer um padrão de uso, com a aplicação de melhores práticas e definições de políticas internas que vão garantir o sucesso e o futuro dos negócios.

REFERÊNCIAS BIBLIOGRÁFICAS

1. **COMO escrever bem:** projeto de pesquisa e artigo científico. Curitiba: Appris, 2018. 186 p., il., 21 cm. (Educação, tecnologias e transdisciplinaridade).
2. COSTA, Marco Antonio F. da. **Projeto de pesquisa:** entenda e faça. 6. ed. Petrópolis, RJ: Vozes, 2015. 140 p., 21 cm. Bibliografia: p. 109-115.
3. **EMPREENDEDORISMO, tecnologia e inovação:** como a tecnologia está transformando a sociedade, a economia e gerando oportunidades para criação de Startups. São Paulo: Livrus, 2015. 199 p., il., 23 cm. Inclui bibliografia. ISBN 9788583601586 (broch.).
4. FERNANDES, Aguinaldo Aragon. **Implantando a governança de TI:** da estratégia à gestão dos processos e serviços. 4. ed Rio de Janeiro: Brasport, 2014. xxviii, 630, il., 23 cm.
5. FERREIRA, Fernando Nicolau Freitas. **Política de segurança da informação:** guia prático para elaboração e implementação. 2. ed., rev. e ampl Rio de Janeiro: Ciência Moderna, 2008. 259p., il., 23 cm. Bibliografia: p. 210-215.
6. LOBO, Edson J. R. **Segurança da informação:** ameaças e controles. Rio de Janeiro: Ciência Moderna, 2019. 183, [1]p., il., 23 cm. Bibliografia: p. [184]. ISBN 9788539909773.
7. MACHADO, Rodrigo Prestes. **Desenvolvimento de software III:** programação de sistemas web orientada a objetos em Java. Porto Alegre: Bookman, 2016. x, 209p., il., 25 cm.
8. MATTOS, João Roberto Loureiro de. **Gestão da tecnologia e inovação:** uma abordagem prática. 2. ed., rev. e atual., 3. tir. São Paulo: Saraiva, 2014. xiii, 433, il., 24 cm. Bibliografia: p. [425]-433. ISBN 9788502178946 (broch.).
9. MENDES, Conceição Maria Carvalho. **Manual de orientações para elaboração de projeto de pesquisa.** Teresina: FUESPI, 2015. 48 p., il., 26 cm. Bibliografia: p. 48. ISBN 9788583200994 (broch.).
10. RÚDIO, Franz Victor. **Introdução ao projeto de pesquisa científica.** 43. ed. Petrópolis, RJ: Vozes, 2015. 144 p., 21 cm. Bibliografia: p. 143-144. ISBN 9788532600271 (broch.).
11. Incidentes reportados ao CERT.br -- Janeiro a Dezembro de 2018. Disponível em: https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html Acessado em: 19 de agosto de 2019.