UNIVERSIDADE DO SUL DE SANTA CATARINA

GUILHERME ANTONIO MACHADO

AVALIAÇÃO DA INTEGRIDADE DOS CONJUNTOS DE DADOS E INFORMAÇÕES:

VISÃO DE USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO

Palhoça

2020

GUILHERME ANTONIO MACHADO

AVALIAÇÃO DA INTEGRIDADE DOS CONJUNTOS DE DADOS E INFORMAÇÕES:

VISÃO DE USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Roberto Fabiano Fernandes

Palhoça

2020

GUILHERME ANTONIO MACHADO

AVALIAÇÃO DA INTEGRIDADE DOS CONJUNTOS DE DADOS E INFORMAÇÕES:

VISÃO DE USUÁRIOS SOBRE SEGURANÇA DA INFORMAÇÃO

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Palhoça, 21 de Junho de 2020.

Prof. e orientador (Roberto Fabiano Fernandes), Ciência da Computação, Especialista em Engenharia e Projetos de Software
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço primeiramente ao professor e orientador Roberto, pelo auxílio prestado. Disponibilizando vídeos, maneiras de melhorar, aprimorar o estudo de caso. Agradeço todas as pessoas que participaram da pesquisa bem como professor Ricardo Assink, auxiliou no aprimoramento da pesquisa para coleta de dados, Ravi, Francisco, colegas de sala de aula, da graduação de Sistemas de Informação. Vinicius colega em comum, participante de um grupo de amigos do curso de SI, e ao Alexandre.

Além dessas pessoas não poderia esquecer de agradecer minha namorada Samara da Silva Motta, meus pais e irmãos que incentivaram.

RESUMO

Este estudo de caso voltado a problemas de integridades de informações de organizações. Com intuito a demonstrar a importância de preservar a integridade de um conjunto de dados, confidenciais dispostas em banco de dados, de empresas estendendo o problema para uso pessoal, que necessitam estar disponíveis com os mecanismos possíveis no meio tecnológico. Conhecido como Pentest®, um teste que é realizado com autorização de acordo com a LEI Nº 12.737, Art. 154ª, e termos para conscientização do ato, mantendo o Pentester livre de problemas. Com finalidade demonstrar as falhas básicas, pertinentes de uma empresa independentemente de qual finalidade, por conta de praticamente ou parcialmente todas organizações demandarem a necessidade do uso da tecnologia. Utilizando com uma pesquisa de caráter exploratório e, com um método de abordagem de pesquisa qualitativa por questionário online. Com cinco pessoas participantes da pesquisa.

Palavras-chave: Redes de Computadores. Gestão da Tecnologia da Informação. Sistemas de Informação.

SUMÁRIO

1 INTRODUÇÃO

Em decorrência a atual pandemia, a tecnologia como um todo, tem sido o movimento a distância entre pessoas, bem como vídeo chamadas, ligações por internet, empresas disponibilizando o único meio de trabalho a distância, com “Home Office” compreendendo a análise, em qualquer ponto a “importância”, de criptografias, de serviços online, sempre disponíveis, e íntegros.

A demanda de pessoas sendo hackeadas em suas contas de “WhatsApp”, por não ter verificação de duas etapas, a ponta de um problema a ser verificado, para a exploração de pessoas mal-intencionadas.

O interesse pelo assunto surgiu quando tinha 15 anos em 2006, meu padrinho Marcelo, apresentou a tecnologia, a partir deste ponto, o interesse abrangeu todos os assuntos ligados a tecnologia da informação. Então ao longo desses 14 anos de experiência com a tecnologia me surgiu o interesse pela segurança da informação.

Estudo mostra a crescente demanda por soluções de serviços de segurança em Tecnologias de Informação, o atual cenário considerando a pandemia, aumento do uso de tecnologias por escolas que até então utilizavam apenas seus meios físicos para entregarem conteúdos de estudos, organizações que tiveram que migrar praticamente todos os seus atendimentos para plataformas online.

Com base no estudo realizado, obtive 83% dentre as cinco pessoas que participaram. Sobre o sistema operacional Kali Linux, a ferramenta selecionada para efetivação da varredura de vulnerabilidades bem como falta de integridade com algoritmos de espelhamento de banco de dados com datas fora do padrão institucional. Disponibilidade passivo a ataques de DDoS. Confidencialidade com criptografias com chaves invalidas.

Este trabalho tem como objetivo apresentar os problemas pertinentes a segurança dos dados transformados em informações, os meios que tramitam esses sistemas organizacionais.

O trabalho foi motivado após observar que existem falhas comuns nas organizações de maneira geral, quando expostas a testes de vulnerabilidades.

2 TEMA

A segurança da informação bem como seu nome traz consigo “segurança” buscar manter o sigilo de informações, bem como manter sempre disponível e confidenciais. E segundo Fraga e Vangller (2017, p. 11) que dizem: “A Segurança da Informação se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa, isto é, aplica-se tanto às 11 informações corporativas quanto às pessoais.”

Estar atento hoje em dia sobre o conteúdo a qual produzimos seja ele um sistema de informação, trabalho acadêmico ou conteúdo digital que, esperamos estar guardado em segurança enquanto a veracidade do que guardamos. Se está sempre disponível, se o conteúdo não foi modificado por um terceiro e, se o conteúdo é confidencial.

Dentre a dúvida, a importância tanto quanto o envolvimento entre organizações, colaboradores das organizações, fornecedores, clientes, ambos conectados por plataformas, estão realmente protegidos ou, estão sendo monitorados em alguma ponta desse mapeamento?

Com o Pentest® é possível analisar falhas contida na organização, conferir se as informações estão sempre disponíveis com o ataque DoS, verificar se são confidenciais, se há falhas comuns na criptografia, bem como a verificação da integridade, se os backups estão constantemente atualizados e preparados com os algoritmos de espelhamentos.

E considero dentre essas falhas o ser humano, em qualquer parte do mapeamento dos processos envolvidos, tanto na parte da produção do algoritmo, quanto na manipulação em qualquer ponto.

Os sujeitos atuantes nessa área de TI podem deixar vestígios, como senhas em mesas de escritório, de sistemas com informações bancárias, tal como, cartões virtuais de transações, informações pessoais de clientes, dando margem a falhas catastróficas. As senhas são portas de entradas para intrusos, a todos dados e informações contidas na empresa.

Um meio de obstruir esse problema, é com treinamentos sobre a atualização de senha a cada dois meses, um mecanismo de autorização pessoal, não manter senhas sobre mesas, bem como o comprometimento com a segurança, demonstrar a importância da cultura e sua responsabilidade estando dentro da organização.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Identificar um método de ataques cibernéticos, em sistemas da informação que comprometam a segurança.

3.2 OBJETIVOS ESPECÍFICOS

- Demonstrar a importância da criptografia em Sistemas de Informação.
- Demonstrar a importância de algoritmos contra-ataques de negação de serviço “DoS”.
- Conseguir demonstrar a importância de espelhamento.
- Identificar. uma política de segurança organizacional.
- Mapear o que pode agregar com os benefícios, no contexto geral, caso implementação ocorra e caso não ocorra.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

O campo de estudo desta pesquisa será feito na universidade UNISUL, localizada na Pedra Branca, Av. Pedra Branca, 25 - Cidade Universitária Pedra Branca, na Cidade de Palhoça, Santa Catarina, cujo CEP é 88137-270, onde há cursos presenciais bem como de Sistemas de Informação, e setor de tecnologia da informação.

Este estudo de caso houve uma pesquisa caracterizada como exploratória, com intuito a explorar a segurança da informação e Cavalcanti, e Moreira (2014, p. 29), que dizem: “Muitas vezes, o pesquisador não dispõe de conhecimento suficiente para formular adequadamente um problema ou elaborar de forma mais precisa uma hipótese. Nesse caso, é necessário”.

Com abordagem qualitativa e Cavalcanti, e Moreira (2014, p. 34), que dizem: “Neste sentido, os pesquisadores fazem suas análises categorizando as expressões coletadas, utilizando instrumentos de coleta de dados, por meio de questionários com questões abertas e/ou entrevistas.”

Contendo questões para respostas elaboradas pelas pessoas que participaram da pesquisa.

Com finalidade garantir com o Pentest® a Disponibilidade, Integridade, Confidencialidade e Política de segurança para que seja possível, o Mapeamento do contexto geral sobre segurança.

4.2 INSTRUMENTOS DE COLETA DE DADOS

Os instrumentos de coleta de dados adotados neste trabalho são descritos no quadro a seguir.

Quadro 1 – Instrumento de coleta de dados

Instrumento de coleta de dados	**Universo pesquisado**	**Finalidade do Instrumento**
Questionário online	Um grupo de estudantes e um professor: No total de 3 pessoas Cargos desempenhados: - Analista e estudante da unisul - Estagiário de Infraestrutura do Call Center e estudante da unisul - Socio Proprietário, e professor da unisul	Garantir com o Pentest® a Disponibilidade, Integridade, Confidencialidade e Política de segurança para que seja possível, o Mapeamento do contexto geral sobre segurança.

Fonte: CAVALCANTI e MOREIRA (2008).

4.2.1 CARACTERIZAÇÃO DA PESQUISA

Este estudo de caso houve uma pesquisa caracterizada como exploratória, com intuito a explorar a segurança da informação e Cavalcanti, e Moreira (2014, p. 29), que dizem: “Muitas vezes, o pesquisador não dispõe de conhecimento suficiente para formular adequadamente um problema ou elaborar de forma mais precisa uma hipótese. Nesse caso, é necessário”.

Com abordagem qualitativa e Cavalcanti, e Moreira (2014, p. 34), que dizem: “Neste sentido, os pesquisadores fazem suas análises categorizando as expressões coletadas, utilizando instrumentos de coleta de dados, por meio de questionários com questões abertas e/ou entrevistas.”

Contendo questões para respostas elaboradas pelas pessoas que participaram da pesquisa.

Com finalidade garantir com o Pentest® a Disponibilidade, Integridade, Confidencialidade e Política de segurança para que seja possível, o Mapeamento do contexto geral sobre segurança.

5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

5.1 DADOS DA ORGANIZAÇÃO

Esta pesquisa foi realizada em uma instituição de ensino superior do estado de Santa Catarina – Universidade do Sul de Santa Catarina (UNISUL). Trata-se de uma instituição de ensino educacional multicampi, de caráter comunitário, fundada em 1964, orientada para produção da educação e desenvolvimento social. Possui cursos de graduação, cursos de pós-graduação *lato e stricto sensu* e cursos de extensão, distribuídos nos seus três campis, denominados Campus Sul, Campus Norte e Campus Virtual.

5.2 ANÁLISE DA REALIDADE OBSERVADA

Este projeto, teve inciativa com a possibilidade explorar se uma organização está protegida, existem técnicas e uma delas chamada Pentest®. Como o próprio nome diz por si, "teste de penetração". Fraga e Vangller (2017, p. 25) que dizem: "objetivo do pentest é o de melhorar a segurança do sistema e da organização por meio das atividades."

Com uso de exploits para acesso aos recursos em sistemas que demonstram vulnerabilidades para serem corrigidos por aquele proprietário que produziu o Sofware testado, rede, infraestrutura, em todos os pontos.

E por se tratar de empresas, tudo deve ser dentro da lei, conforme "LEI Nº 12.737, Art. 154A" contida no site do Planalto:

Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. (BRASÍLIA, 2012)

E de acordo com a lei todos os procedimentos que forem efetuados devem estar explícitos com autorização expressa ou tácita do titular da organização ou empresa que for exposta ao pentest®, de acordo com o contrato de serviço que for determinado no ato da contratação do serviço, prevendo assim expressamente a exclusão de eventual incidente dentro da LEI Nº 12.737, Art. 154A.

Esse contrato de serviço intitulado NDA, "acordo de não divulgação" confidencialidade de empresa, contratante para o contratado do serviço, não haver vazamento de informações.

A seguir alguns tópicos sobre assuntos relevantes a segurança bem como:

INTEGRIDADE

Para se manter integro, em um cenário onde identifiquei com a pesquisa, capaz de reduzir e não ausentar a capacidade de uma pessoa realizar testes de penetração, porém há

maneiras relativamente seguras como o backup de segurança, conforme a resposta do professor Ricardo Assink quando diz ser Necessário contingência, espelhamento de servidor, sistema de autenticação confiável e devidamente configurado.

Moraes (2015, p. 21) diz que “A integridade é o serviço de segurança que garante que a informação não será alterada, intencionalmente ou não, durante seu armazenamento ou processamento. Garantir a integridade é uma tarefa fundamental.”

DISPONIBILIDADE:

Oitenta e três porcento das pessoas que participaram da pesquisa, consideraram extremamente importante, o fato que dados transformados em informações e considerando o fato que Moraes (2015, p. 21) diz que: "Negação de Serviço, os famosos DoS (Denial of Service), O objetivo desses ataques é tornar um determinado serviço indisponível."

De acordo com o uso legítimo do proprietário do conteúdo, o produziu, podendo ser indisponibilizado por uma segunda pessoa, seja ele um servidor, data center, ou propriedades intelectuais, bem como computadores e com intuito a quebra de disponibilidade.

CONFIDENCIALIDADE:

Para tornar um banco de dados confidencial, existe uma técnica antiga chamada criptografia, usada em guerras para decifrar comunicação de ponta a ponta, uma tarefa bem complexa e amplamente probabilísticas, Criptografia é uma camada adicional na proteção de dados sigilosos é que necessitam de alto nível de segurança.

Para a proteção de Dados de senhas, criptografia se torna imprescindível, assim como englobar conteúdos junto como cadastros de pessoas, acessíveis apenas aos proprietários do conteúdo e aos administradores para manutenção, de algum nível.

Moraes (2015, p. 21) diz que: “A confidencialidade é o serviço de segurança que garante que apenas usuários autorizados tenham acesso à informação.”

POLÍTICA DE SEGURANÇA

Atualmente política de segurança nas organizações bem como mecanismos físicos, como trancas de portas contendo senhas, política de treinamento de colaboradores, responsabilidade da área de TI, com a implementação dos controles necessários para cumprir os requerimentos de segurança estabelecidos pela política de segurança da informação.

Treinamento com as pessoas para se adequarem à política de segurança imprescindivelmente importante, a responsabilidades dos colaboradores, responsabilizações em caso de má utilização dos recursos de TI da empresa.

MAPEAMENTO NO CONTEXTO GERAL SOBRE SEGURANÇA:

De acordo com a pesquisa realizada, o professor Ricardo Assink responde à pergunta sobre o mapeamento, diz que: Quando todos os níveis de segurança são implementamos o risco em perda de dados, sobretudo os sigilosos, diminui substancialmente. Então cada or-

ganização deve avaliar as reais necessidades da implementação de todos os níveis levando em consideração o valor agregado da informação que deve ser protegida.

Contudo, os dados sigilosos, bem como senhas, nível de segurança em camadas para cada pessoa, garantindo a confidencialidade, integridade, disponibilidade bem como a política de segurança. Dependendo do sistema, da organização, deve ser feito uma análise detalhada de cada componente, bem como Financeiro, Recursos Humanos, Logística, Central de Relacionamento. Setores que trabalham diretamente com informações pessoais, de clientes, funcionários, logo diminuiu substancialmente os riscos de perda de recursos financeiros.

Caso não ocorra, o problema exposto poderá acarretar problemas catastróficos, financeiramente, perda de clientes, bem como a quebra de confidencialidade que deve se manter entre cliente e empresa.

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

Dentre a dúvida, se uma empresa ou organização está segura, junto a importância do envolvimento direto entre organizações, considerando entre colaboradores das organizações, fornecedores com organizações, clientes, ambos conectados por plataformas, estão realmente protegidos por barreiras bem como algoritmos atualizados ou, estão sendo monitorados em alguma ponta desse mapeamento ponta a ponta?

Monitorando para vantagens pessoais ou empresariais, bem como inteligência competitiva.

Identifiquei como problema, a situação crítica de algumas empresas que não estão adequadas quanto à segurança básica, seja ela lógica, física, políticas de segurança, envolvendo pessoas, Sistemas de informações, banco de dados logo transformado em informações sigilosas e confidenciais.

Capazes de levar uma organização a um colapso, ocorrendo o mapeamento de fatores que podem aumentar a segurança ou diminuir por falta de Integridade, disponibilidade e confidencialidade dos dados gerados, ou armazenados e por falta de política de segurança, bem como treinamentos e responsabilidades dos colaboradores por estarem trabalhando com informações de responsabilidade empresarial.

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

A técnica selecionada, junto ao sistema operacional Kali Linux, com a ferramenta correta, identifiquei com a pesquisa levantada, que os participantes escolheram o NMAP, a chamando de uma maneira formal como “Canivete Suíço”, onde é testado as vulnerabilidades mais comuns, aplicado em uma rede. Um servidor seguro, deve no mínimo, “sobreviver” aos testes padrão do Pentest.

Uma das características da ferramenta é identificar falhas comuns, realizando uma varredura com o NMAP, utilizando o Sistema operacional Kali, mantendo uma segurança básica. Dados transformados em informações íntegros com o uso do backup em espelhamento. Confidenciais com a criptografia e em plena disponibilidade, criando barreiras contra-ataques de Negação de Serviços.

Além de minicursos para conscientização dos funcionários e suas responsabilidades quanto ao tratamento das informações. De acordo com a necessidade de cada organização, com as políticas definidas pela empresa ou organização.

6.2 RESULTADOS ESPERADOS

O resultado esperado é que todos os mecanismos de defesa, reduzam os ataques. Mantendo informações integras, disponíveis e confidenciais e custos agregados que possivelmente possa ter, porém reduzidos.

6.3 VIABILIDADE DA PROPOSTA

a. Implementação de espelhamento de Backup
    - Redundância de servidores preparados por algoritmos para serem utilizados caso baixe principal.
    - Algoritmo de “hashing” para detectar possíveis erros.
b. Criptografia de sistemas de autenticação de ponta a ponta,
    - Identificação da autenticidade de uma determinada mensagem.
    - Encriptação de informações por meio de cifragem.
    - Criação de chaves criptográficas.
c. Algoritmo contra DDoS (Distributed Denial of Services).
    - Disponibilidade contra ataques de negação de serviços.
    - Desvio de negação de serviço.

7 CONSIDERAÇÕES FINAIS

O conteúdo aqui disponibilizado, foi incentivado por problemas generalistas bem como a segurança, um insumo que qualquer organização deve se ater, manter os sigilos necessários de um conjunto de processos elaborados.

Estejam de acordo com os planos de negócios, bem como o planejamento estratégico de longo prazo, planejamento tático de médio prazo e o planejamento operacional, com os processos de curta duração, manter todos os insumos de informação organizacionais intactos, sempre disponíveis e confidenciais.

A pesquisa levantada é de suma importância pois, se obtém uma visão diferente de pessoas, contribuindo com possíveis soluções.

REFERÊNCIAS

BRASÍLIA. Dilma Rousseff. Presidência da República Casa Civil. **LEI Nº 12.737**: DE 30 DE NOVEMBRO DE 2012. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 01 jun. 2020.

CAVALCANTI, Marcelo e MOREIRA, Enzo. **Metodologia de estudo de caso**: livro didático. 3. ed. rev. e atual. Palhoça: Unisul Virtual, 2008. 170 p.

ELIANE. **10 dicas das ferramentas de pentesters mais usadas no mercado**. Disponível em: <https://www.3way.com.br/conheca-10-ferramentas-usadas-por-pentesters/>. Acesso em: 08 Abr 2020.

FRAGA, Bruno; VANGLLER, Thompson. **Técnicas de invasão: aprenda as técnicas usadas por hackers em invasões reais.** Aprenda as técnicas usadas por hackers em invasões reais. Londres: Beatriz Amoedo Giorgi, 2017.

MORAES, de, Alexandre Fernandes. **Firewalls - Segurança no Controle de Acesso.** São-Paulo; Editora Érica Ltda, 2015. 9788536521978. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788536521978/. Acesso em: 08 Abr 2020.