CENTRO UNIVERSITÁRIO UNIFECAF
GESTÃO TECNOLOGIA DA INFORMAÇÃO

Dannyelly Dayane Queiroz

DESAFIO DE SEGURANÇA CIBERNÉTICA: AUMENTANDO A CONSCIENTIZAÇÃO E A PROTEÇÃO DIGITAL EM AMBIENTES CORPORATIVOS

Taboão da Serra,
SP 2024

DANNYELLY DAYANE QUEIROZ

DESAFIO DE SEGURANÇA CIBERNÉTICA: AUMENTANDO A CONSCIENTIZAÇÃO E A PROTEÇÃO DIGITAL EM AMBIENTES CORPORATIVOS

Trabalho apresentado como requisito parcial de avaliação da disciplina **Cyber Security** do Curso de Graduação em **Gestão Tecnologia da Informação** do Centro Universitário UniFECAF.

Tutor(a): **Fernando Leonid**

Taboão da Serra,

SP

SUMÁRIO

LISTA DE ABREVIATURAS

CIA - Confidencialidade, Integridade e Disponibilidade

DBIR - Data Breach Investigations Report

GDPR - General Data Protection Regulation

ISO/IEC - International Organization for Standardization / International Electrotechnical Commission

LGPD - Lei Geral de Proteção de Dados

MFA - Multifactor Authentication

NIST - National Institute of Standards and Technology

ERP - Enterprise Resource Planning

CRM - Customer Relationship Management

DDoS - Distributed Denial of Service

TI - Tecnologia da Informação

PDF - Portable Document Format.

1. INTRODUÇÃO

A FecafTECH é uma empresa inovadora de tecnologia que, nos últimos meses, enfrentou uma série de incidentes de segurança, muitos dos quais foram causados por erros humanos, como o clique em links suspeitos, o uso de senhas fracas e o compartilhamento não autorizado de informações confidenciais. Esses incidentes demonstram uma vulnerabilidade crescente na organização, principalmente devido à falta de conscientização dos colaboradores sobre práticas de segurança. Isso é ainda mais preocupante diante do aumento de ataques de que se aproveitam da falta de preparação dos usuários para comprometer sistemas e dados valiosos.

Diante dessa situação, a diretoria da FecafTECH reconheceu que um dos maiores desafios da empresa não está apenas na tecnologia, mas na educação e treinamento de seus colaboradores. A conscientização sobre segurança cibernética é um fator crucial para reduzir esses riscos, garantindo que todos na organização compreendam os perigos e saibam como se proteger adequadamente. Sendo assim, fui contratado como consultor de segurança cibernética para elaborar um plano que vise melhorar o nível de conscientização e adotar práticas mais seguras dentro da empresa.

Este trabalho tem como objetivo apresentar um plano de conscientização em segurança Cibernética, com foco nas necessidades da FecafTECH. O plano será estruturado em três partes principais: um diagnóstico inicial do atual nível de conscientização sobre segurança entre os colaboradores, a proposta de ferramentas e estratégias para promover a proteção de dados e a criação de um programa de treinamento contínuo que incentive uma verdadeira cultura de segurança digital.

Neste contexto, é fundamental compreender que a segurança cibernética não depende apenas de tecnologia, mas também por parte dos funcionários. A conscientização é, portanto, a chave para transformar a postura de segurança da FecafTECH e minimizar as ameaças internas e externas.

1.1.Contextualização do problema

No contexto atual, as empresas dependem da segurança da informação para proteger o seu bem mais precioso: dados. Desde informações financeiras a registros pessoais de clientes, qualquer vulnerabilidade pode resultar em perdas financeiras, danos à reputação ou até mesmo em sanções legais.

Com o avanço das ameaças digitais, como ataques de phishing e engenharia social, muitas organizações enfrentam desafios significativos para proteger suas informações. Apesar do investimento em tecnologia de ponta e sistemas avançados de segurança, o fator humano continua sendo uma das maiores vulnerabilidades no ambiente corporativo.

Na FecafTECH, incidentes recentes expuseram problemas graves relacionados ao comportamento dos colaboradores. O uso de senhas fracas, cliques em links maliciosos e o compartilhamento inadvertido de informações confidenciais indicam uma falta de conscientização em relação às práticas de segurança cibernética. Esses erros humanos têm impactos graves, comprometendo não apenas a integridade dos dados corporativos, mas também a reputação da empresa e sua capacidade de competir em um mercado altamente tecnológico.

E esse cenário se repetem em muitas empresas, na qual a falta de treinamento e de uma cultura organizacional voltada para a segurança resulta em falhas que poderiam ser evitadas. De acordo com o relatório de Investigações de Violação de Dados da Verizon (DBIR) de 2024, destacam que a engenharia social e o phishing continuam sendo as principais causas de violações de segurança, reforçando a importância de se investir em treinamento para mitigar esses riscos.

E normas internacionais como a ISO/IEC 27001 27001 e as diretrizes do NIST (National Institute of Standards and Technology), apontam a conscientização como um pilar essencial para a segurança da informação.

Na FecafTECH, a ausência de uma cultura de segurança eficaz representa um risco significativo, tanto em termos de perdas financeiras quanto de danos à confiança dos clientes. Desta forma, é fundamental a implementação de um plano de conscientização e treinamento para seus colaboradores, promovendo comportamentos seguros e reduzindo a exposição às ameaças digitais.

No presente trabalho buscamos atender essa necessidade, oferecendo uma solução estruturada e eficaz para fortalecer a segurança cibernética e proteger os ativos da FecafTECH.

2. Objetivo do plano de conscientização

O objetivo principal do plano de conscientização para a FecafTECH é criar uma cultura organizacional que valorize e entenda a importancia da segurança da informação sendo um aspecto essencial do dia a dia corporativo.

E para reduzir a probabilidade de incidentes de segurança, como vazamentos de dados, ataques cibernéticos e perda de informações confidenciais, vamor seguir com objetivos

especificos, sendo eles:

- Promover a conscientização sobre a importância da segurança da informação em todos os níveis da organização.
- Minimizar a probabilidade de incidentes como vazamentos de dados, ataques cibernéticos e perda de informações confidenciais.
- Implementar medidas para proteger os ativos de informação da empresa, incluindo dados confidenciais e propriedade intelectual.
- Garantir o cumprimento da LGPD e de outras regulamentações pertinentes à proteção de dados.
- Proteger a imagem da FecafTECH e a confiança de clientes, parceiros e stakeholders.

2.1.Pessoas afetadas

A falta de conscientização em segurança cibernética pode afetar diversos setores e níveis de uma empresa, prejudicando não apenas os funcionários, mas também outros stakeholders, como gestores, clientes, fornecedores e investidores. Essa falta de preparação torna a empresa vulnerável a uma série de ataques cibernéticos que podem ter consequências graves e de longo prazo. A seguir vamos detalhar cada um:

- Funcionários: Os funcionários são o grupo mais diretamente afetado pela falta de conscientização em segurança cibernética. Isso ocorre principalmente porque eles representam o elo mais fraco na cadeia de segurança da informação. Muitos ataques cibernéticos, como o phishing, dependem de enganar o funcionário para que ele forneça dados sensíveis ou clique em links maliciosos. A falta de treinamento adequado e a falta de conhecimento sobre práticas seguras deixam os colaboradores vulneráveis a cometer erros.

- Clientes: Os clientes são impactados diretamente pela falta de segurança cibernética principalmente quando seus dados pessoais e financeiros são comprometidos pela empresa.

- Setor de TI: O setor está diretamente afetado pela falta de conscientização em segurança cibernética, pois são os responsáveis pela proteção e manutenção da infraestrutura tecnológica da empresa. E quando os funcionários não estão preparados ou informados sobre as melhores práticas de segurança, as medidas implementadas pela equipe de TI podem ser comprometidas, tornando-se ineficazes.

3. FUNDAMENTAÇÃO TEORICO

3.1. Diferenças entre dados e informação

Dados e informação são conceitos fundamentais na era digital. Segundo Setzer, “definimos dado como uma representação simbólica (isto é, feita por meio de símbolos),

quantificada ou quantificável". Ou seja, dados são representações de fatos ou ideias que podem ser medidas ou contadas. Um texto, uma imagem ou um número são exemplos de dados.

A informação, por sua vez, é o resultado do processamento e interpretação dos dados. Dados brutos, muitas vezes isolados, ganham significado quando são organizados, analisados e contextualizados. Esse processo transforma dados em conhecimento útil para a tomada de decisões.

Um banco de dados, segundo Dante (2000), é uma coleção organizada de dados persistentes, utilizados por sistemas de informação. É como um depósito de dados, onde as informações são armazenadas de forma estruturada para facilitar o acesso e a recuperação.

Galvão (2015) complementa essa ideia ao afirmar "os dados são os elementos brutos, enquanto as informações são o resultado do processamento desses dados pelo computador."

Portanto, os dados são a matéria-prima da informação. Ao organizar, analisar e interpretar os dados, obtemos insights valiosos que podem ser utilizados para resolver problemas e tomar decisões.

3.2. Importância da Proteção de Dados: Segurança da Informação~~[DQ1]~~

A afirmação de que "dados são o novo petróleo" creditada ao matemático Clive Humby, sendo justificada com a continuação "assim como o petróleo, os dados são valiosos, mas se não forem trabalhados adequadamente, não podem ser realmente usados em aplicações comerciais, da mesma forma que o petroleo bruto não é utilizado diretamente", essa frase reflete atualmente o quão importante são os dados.

Contudo, essa valorização também aumentou a exposição a riscos, como vazamentos, roubos e acessos não autorizados, que podem comprometer a privacidade e a segurança de organizações.

Portanto, é importante implementar medidas de segurança robustas e seguir regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção de Dados (GDPR) na Europa. Além disso, temos instituições como o Instituto Nacional de Padroes e Tecnologia (NIST) desempenham também um papel fundamental, ao estabelecer diretrizes e boas praticas para a proteção dos dados.

3.2.1. Principios da segurança

A segurança é guiada por três pilares principais, conhecidos como Tríade CIA (Confidencialidade, Integridade e Disponibilidade), além de outros conceitos complementares que garantem a proteção eficaz das informações.

Segundo Solomon (2014) "uma brecha de segurança pode ser definida como qualquer evento que resulte em uma violação de qualquer um dos princípios de segurança:

disponibilidade, integridade e disponibilidade."

Desta forma, podemos dizer que a segurança da informação foi caracterizada na criação de políticas e metodologias para que a proteção das informações não ficasse em risco. A seguir, veremos os princípios da segurança, ela introduz três objetivos principais que são conhecidos como a tríade CIA (do acrônimo em inglês para confidentiality, integrity and availability).

3.2.1.1. Confidencialidade

De acordo com Galvão (2015), "a confiabilidade consiste, portanto, em garantir que apenas pessoas autorizadas tenham acesso ao conteúdo. [...] o método mais utilizado para prover confiabilidade a uma informação é a autenticação de acesso"

A citação de Galvão (2015) destaca um dos aspectos fundamentais da confiabilidade da informação, que envolve garantir que apenas indivíduos autorizados possam acessar determinado conteúdo. Em termos de segurança da informação, isso se traduz na autenticação de acesso, que é o processo de verificar a identidade de uma pessoa ou sistema antes de conceder acesso a dados ou serviços sensíveis.

A autenticação de acesso pode ser realizada por meio de várias maneiras, como senhas, biometria, tokens, ou sistemas de autenticação multifatorial. O objetivo é assegurar que somente aqueles que têm permissão possam interagir com as informações e/ou sistemas protegidos, minimizando os riscos de acessos não autorizados ou manipulação indevida dos dados.

3.2.1.2. Integridade

Segundo Galvão (2015), "o princípio da integridade se baseia na garantia de que informações armazenadas estão corretas, são verdadeiras e não sofreram nenhum tipo de violação, isto é, que qualquer alteração, redução ou acréscimo foram autorizados por seus proprietários."

Ou seja, qualquer alteração, adição ou remoção de dados deve ser realizada com o devido consentimento e autorização dos proprietários dessas informações.

É essencial para garantir a confiança nas informações manipuladas em sistemas de dados, assegurando que os dados não foram corrompidos, alterados indevidamente ou expostos a manipulações externas não controladas pela empresa. O princípio da integridade contribui para a proteção contra fraudes, erros e acessos não autorizados, sendo vital para a segurança e a confiabilidade de sistemas informáticos, bancos de dados, e até transações digitais.

Em termos de aplicação para garantir a integridade das informações envolve-se o uso de ferramentas como criptografia, verificações de integridade e protocolos de autorização para garantir que apenas pessoas autorizadas possam realizar modificações nas informações.

3.2.1.3. Disponibilidade

A citação de Galvão (2015) destaca, “a disponibilidade é a garantia de que as informações estarão disponíveis sempre que forem solicitadas pelas pessoas autorizadas. [...] o principio da disponibilidade está diretamente relacionado a eficácia dos sistemas que armazenam tais informações, isto é, dependem intrinsicamente do bom funcionamento desses sistemas.”

Esse principio implica que as informações precisam estar prontamente disponíveis ou acessiveis quando requeridas, sem interrupções ou atrasos que possam comprometer a eficácia dos processos que dependem desses dados, permitindo que os processos dependentes dessas informações possam ocorrer de maneira fluida e eficiente. Portanto, o princípio da disponibilidade envolve a manutenção de uma infraestrutura de TI confiável e resiliente, que seja capaz de assegurar o acesso contínuo às informações.

Além da tríade, acrescentaram-se outros aspectos importante para a segurança da informação.

3.2.1.4. Autenticidade

A autenticidade garante a credibilidade e a confiança nos sistemas, assegurando que a identidade do usuario ou a veracidade de uma mensagem sejam verificáveis e confirmadas.

Conforme Silva (2023) “é a garantia de que num processo de comunicação os remetentes sejam exatamente o que dizem ser e que a mensagem ou informação não foi alterada após o seu envio ou validação.”

3.2.1.5. Irrevogabilidade

A irrevogabilidade assegura que uma vez que uma ação foi realizada, ela não pode ser negada ou alterada de forma a invalidá-la, o que promove a responsabilidade e confiança nas transações ou nos registros feitos. A irrevogabilidade é um princípio fundamental para garantir a responsabilidade e a segurança jurídica das informações, evitando fraudes, manipulação de informações e ações deliberadas para reverter compromissos assumidos ou decisões tomadas.

Conforme Galvão (2015) cita , “o principio da irrevogabilidade existe para que não seja possivel negar um ato. Uma vez que a informação existe e é autentica esse principio garante que ela seja irrevogavel, ou em um termo mais simples, inegavel.”

4. Ameaça

Entendamos como ameaça todo e qualquer fator capaz de, eventualmente, causar um incidente ou problema que possa prejudicar uma organização de alguma forma.Podemos considerar como ameaça, agentes ou condições que geram incidentes que afetam a integridade das informações e outros ativos, por meio da exploração de vulnerabilidades, provocando

perdas que causem impactos aos negócios da empresa (SÊMOLA, 2003).

Ao tratar da definição de ameaça, é fundamental compreender que ela pode se manifestar de diversas formas, seja por meio de ataques externos, como hackers ou vírus, ou através de vulnerabilidades internas, como erros humanos ou falhas de infraestrutura tecnológica. A exploração dessas falhas pode comprometer a segurança das informações sensíveis, como dados financeiros, informações pessoais de clientes ou registros confidenciais de funcionários, o que pode gerar impactos negativos tanto financeiros quanto operacionais.

O conceito de ameaça está diretamente relacionado à identificação de vulnerabilidades na infraestrutura da organização. Quando uma vulnerabilidade é identificada, ela se torna um ponto de exploração tornando a organização suscetível a ataques que podem comprometer a confidencialidade, integridade ou disponibilidade das informações.

As ameaças à segurança podem ser distribuidas em tres categorias sendo elas: confidencialidade, integridade e disponibilidade.

- **Perda de confidencialidade:**

Ocorre quando informações confidenciais são expostas a pessoas não autorizadas.

Exemplo: Vazamento de senhas em sites.

- **Perda de integridade:**

Acontece quando dados são manipulados ou alterados por indivíduos não autorizados, ou usados de forma indevida.

Exemplo: Alteração intencional ou indevida de informações importantes.

- **Perda de disponibilidade:**

Sucede quando informações ou sistemas se tornam inacessíveis para pessoas autorizadas.

Exemplo: Interrupção de comunicação com um servidor essencial devido a falhas ou ataques.

4.1.Tipos de ataques

Os ataques em segurança da informação são tentativas maliciosas de comprometer a confidencialidade, integridade ou disponibilidade de sistemas, redes, ou dados, com o intuito de obter acesso não autorizado, causar danos ou obter vantagens indevidas. Esses ataques podem variar em complexidade e objetivo, mas, em geral, têm o propósito de explorar vulnerabilidades em sistemas de segurança para realizar atividades prejudiciais ou ilegais.

4.1.1. Ataque passivo

Conforme Silva, “um ataque passivo possui como objetivo a descoberta ou a utilização de informações do sistema atacado sem afetar os recursos desse sistema.” Ou seja, o objetivo

de um ataque passivo é monitorar ou espionar um sistema, buscando obter informações de forma furtiva e sem ser detectado, sem alterar ou prejudicar os dados ou recursos do sistema atacado.

Isso significa que, ao contrário dos ataques ativos, que causam modificação ou interrupção nos dados, os ataques passivos se limitam a coletar informações sem deixar rastros visíveis.

Um exemplo clássico de ataque passivo é a captura de pacotes de dados que estão sendo transmitidos pela rede. Nesse tipo de ataque, o atacante intercepta os pacotes de dados que circulam pela rede, sem alterar nada no conteúdo da comunicação, mas coletando informações confidenciais. Esse processo pode envolver a captura de informações como senhas, números de cartões de crédito, dados bancários, ou até credenciais de acesso para outros sistemas. Além deste, outro exemplo é o ataque de sniffing, em que o invasor utiliza ferramentas de "sniffing" para monitorar o tráfego de rede, interceptando dados sem modificar ou alterar qualquer informação. O atacante pode capturar informações como e-mails, senhas e outros dados pessoais, sem que a vítima perceba.

4.1.2. Ataque ativo

Os ataques ativos envolvem interferência direta no fluxo de dados ou nos sistemas de comunicação, com a intenção de modificar, interromper ou manipular informações.

Conforme afirmado por Silva, nos ataques ativos, "ocorre modificação no fluxo de dados ou criação de fluxo falso". Isso significa que o atacante pode alterar as informações transmitidas, interromper a transmissão legítima de dados ou até criar dados falsificados para enganar o sistema ou os usuários. Esse ataque pode causar consequências graves, como: destruição de dados, acesso não autorizado ou interrupção de serviços.

Um exemplo clássico de ataque ativo é o DDoS (Distributed Denial of Service). Nesse tipo de ataque, o atacante controla um grande número de dispositivos infectados, formando uma botnet (rede de dispositivos comprometidos). Esses dispositivos são usados para gerar um tráfego massivo de dados em direção a um servidor ou rede alvo. Como o tráfego malicioso vem de múltiplas fontes distribuídas, o ataque se torna mais difícil de detectar e bloquear, já que o tráfego não provém de um único ponto de origem. O principal objetivo de um DDoS é tornar o sistema ou serviço alvo indisponível para os usuários, seja por sobrecarga de tráfego ou interrupção no processamento de requisições. O tráfego malicioso gerado por um DDoS pode ser tão volumoso que sobrecarrega os servidores, resultando em uma interrupção de serviços, perda de dados ou dano à reputação da organização afetada. Outro exemplo de ataque ativo é o phishing onde o atacante tenta enganar a vítima para que ela forneça informações como

senhas ou dados bancários, geralmente através de e-mails ou sites falsificados.

O atacante pode criar uma página de login falsa, por exemplo, para capturar as credenciais da vítima, comprometendo assim a confidencialidade e segurança do sistema

5. DIAGNÓSTICO INICIAL DA FECAFTECH

5.1.Fatores Contribuintes para as Vulnerabilidades

A FecafTech enfrentou uma série de incidentes de segurança que comprometeram a integridade de seus dados. Após uma investigação interna, ficou evidente que esses incidentes foram, em grande parte, causados por erros humanos.

Erros como cliques em links suspeitos, uso de senhas fracas e o compartilhamento não autorizado de informações confidenciais destacaram a falta de conscientização entre os colaboradores, o que se mostrou uma das principais causas das vulnerabilidades da empresa.

Diante desses erros, foram identificados os seguintes problemas:

- Baixo conhecimento sobre riscos cibernéticos: A maioria dos colaboradores não reconhece e-mails fraudulentos ou links suspeitos.
- Práticas de senha frágeis: Muitos utilizam senhas fáceis de adivinhar e repetem as mesmas credenciais em diferentes plataformas.
- Ausência de treinamento estruturado: Não há programas regulares para educar os colaboradores sobre boas práticas de segurança.

6. PROPOSTA DE FERRAMENTAS E ESTRATÉGIAS

O objetivo dos treinamentos é conscientizar os colaboradores sobre os riscos cibernéticos, como phishing, engenharia social e o uso de senhas fracas. O treinamento será realizado regularmente, de forma presencial ou online, com o uso de material interativo, como quizzes, estudos de caso e questionários, que incentivam o aprendizado prático.

O conteúdo do treinamento abrange diversos temas cruciais para a segurança cibernética, como a identificação de e-mails fraudulentos, links suspeitos, e as táticas de engenharia social. Também serão abordadas as práticas de criação de senhas fortes, a importância da autenticação multifatorial (MFA) e a proteção de dados sensíveis no ambiente corporativo.

A periodicidade do treinamento é essencial para garantir sua eficácia. Todo colaborador passará por um treinamento inicial durante o processo de integração na empresa. Após isso, serão realizadas reciclagens periódicas a cada 3 meses para manter os colaboradores atualizados sobre as novas ameaças.

A empresa adotará o "Mês da Segurança", em outubro, com atividades intensivas focadas na segurança cibernética, como workshops, treinamentos especializados, desafios

interativos e discussões sobre as melhores práticas de proteção. O Mês da Segurança irá culminar com uma grande palestra ou evento com profissionais renomados da área de segurança cibernética para reforçar a importância da segurança na empresa, com uma abordagem divertida e educativa, envolvendo todos os setores da empresa.

7. PROGRAMA DE CONSCIENTIZAÇÃO E TREINAMENTO

O programa terá como objetivo educar e conscientizar os colaboradores da empresa sobre as práticas seguras e o uso seguro da rede, para reduzir os riscos de incidentes na empresa e promover uma uma cultura de segurança na FecafTech.

Ele será dividido em 4 partes, sendo elas: treinamento inicial, treinamento periodico, atividades continuas de conscientização e o mês da cybersegurança.

7.1.Treinamento inicial

Todo colaborador passará por um treinamento incial durante o processo de integração na empresa para entender as diretrizes e politicas de segurança da FecafTech.

7.1.1. Atividades

- Introdução à segurança cibernética e às políticas internas.
- Identificação de ameaças como phishing, engenharia social e malwares.
- Política de criação para senhas seguras.
- Uso correto de ferramentas como autenticação multifatorial (MFA)

7.2.Treinamento periódico

A cada 3 meses, os colaboradores participarão de sessões de reciclagem para reforçar os conceitos, atualizar sobre novas ameaças cibernéticas e garantir que as práticas de segurança estejam sendo corretamente aplicadas no ambiente de trabalho.

7.2.1. Atividades:

- Workshops práticos com estudos de caso recentes.
- Simulações de ataques cibernéticos, como campanhas controladas de phishing e análises de incidentes simulados, com exemplos de casos reais.
- Exercícios interativos, como quizzes e desafios em equipe.
- Realização de quizzes mensais com perguntas relacionadas à segurança cibernética.
- Palestras para que colaboradores saibam como relatar e reagir a incidentes de segurança.

7.3. Avaliação de Feedback

Durante os treinamentos periodicos, os supervisores ou gestores, observarão a participação ativa e a aplicação prática dos conceitos. Após cada sessão, serão analisados os resultados das avaliações e quizzes para identificar lacunas de aprendizado.

Cada colaborador receberá um retorno individual sobre seu desempenho nas atividades e orientações específicas para melhoria. E para os colaboradores que demonstrarem um alto nível de conscientização, serão ofertados incentivos como prêmios. Os colaboradores que obtiverem as maiores pontuações serão premiados com brindes ou certificados de reconhecimento, incentivando a participação dos colaboradores a participar dos treinamentos.

7.4.Atividades Contínuas de Conscientização

Para reforçar a cultura de segurança cibernética de forma contínua, serão implementadas atividades na FecafTech para promover o aprendizado constante e o engajamento dos colaboradores.

7.4.1. Atividades

- Envio de boletins por email com dicas de segurança - atualizações sobre novas ameaças cibernéticas e orientações práticas para os colaboradores.

- Envio por email de simulações de phishing - para testar a capacidade dos colaboradores de identificar e-mails fraudulentos.

- Criação de materiais com mensagens educativas e ilustrações simples, espalhados em áreas comuns, como corredores, refeitórios e pontos de acesso aos sistemas.

- Exemplos: lembretes sobre não compartilhar senhas, reconhecer e-mails fraudulentos ou a importância de bloquear a tela ao sair da estação de trabalho.

- Envio de quizzes e games com pontuação, para reforçar e conscientizar sobre as ameaças, além de promover o aprendizado, retribuir aos colaboradores quem tiver com pontuação maior receberá brindes.

7.5.Ferramentas para os treinamentos

Para realizar treinamentos sobre segurança cibernética, existem várias ferramentas que podem ser úteis. Essas ferramentas ajudam a educar os usuários sobre como prevenir ataques cibernéticos, como phishing, engenharia social, malware, e outros riscos.

Para a FecafTECH, vamos usar a Cyber Risk Aware, uma plataforma que se concentra em educar os funcionários sobre segurança cibernética, com foco na conscientização e prevenção de ataques.

A plataforma oferece: Treinamentos de conscientização, Simulações de phishing, Gestão de riscos e Treinamentos personalizados

8. POLITICA DE SENHAS

8.1.Segurança de senhas

Conforme Silva (2023), “é importante usar senhas fortes para proteger dispositivos de rede.” Para melhorar a segurança das contas dos colaboradores, especialmente nas que

possuem acesso a sistemas críticos, é essencial adotar uma política rigorosa de senhas fortes e autenticação multifatorial (MFA).

Primeiramente, é essencial estabelecer uma política rigorosa de senhas fortes, que defina requisitos claros para a criação de senhas complexas e únicas. Isso inclui a exigência de senhas com combinações de letras maiúsculas e minúsculas, números e caracteres especiais, com um comprimento mínimo recomendado de 12 a 16 caracteres. Além disso, é importante promover o uso de gerenciadores de senhas para que os colaboradores possam armazenar suas credenciais de forma segura, evitando a reutilização de senhas em múltiplas plataformas.

Além disso, a implementação de MFA deve ser obrigatória para todas as contas críticas, adicionando uma camada extra de segurança. O MFA pode ser feito através de códigos temporários enviados para o celular ou tokens gerados por aplicativos como o Google Authenticator, dificultando o acesso não autorizado, mesmo que a senha seja comprometida.

8.1.1. Requisitos para Senha FecafTech:

Uma política de senha é um conjunto de regras e restrições que visam aumentar a segurança e incentiva os usuários a usarem senhas fortes. Assim, vamos seguir as políticas, segundo as diretrizes do NIST (National Institute of Standards and Technology), publicadas no NIST Special Publication 800-63B.

8.1.1.1.Comprimento da Senha

As senhas devem ter no mínimo 8 a 16 caracteres para usuários e até 20 caracteres para administradores. Senhas mais longas são mais difíceis de quebrar por ataques de força bruta.

8.1.1.2.Requisitos Rígidos de Complexidade

Exigirimos combinações caracteres especias, letra maiuscula e minuscula.

8.1.1.3.Uso de Gerenciadores de Senhas

É obrigatório o uso de gerenciadores de senhas, como o Bitwarden, para o armazenamento seguro de credenciais. O uso de senhas simples em múltiplas plataformas ou sistemas será monitorado. Caso identificado, o colaborador receberá um email informando que a senha deverá ser alterada.

8.1.1.4.Autenticação Multifatorial (MFA)

O MFA será obrigatório para todas as contas de sistemas críticos, como ERP, CRM e plataformas de dados sensíveis e será configurado imediatamente após o primeiro acesso ao sistema.

A autenticação pode ser feita por código temporário enviado utilizando aplicativos

como Google Authenticator.

8.1.1.5.Alteração de Senhas

Alterações periódicas de senhas serão exigidas. As senhas precisarão ser alteradas a cada 90 dias.

8.1.1.6.Verificação de Força da Senha

Será implementada uma ferramenta para verificar a força da senha durante a criação ou alteração, ajudando os usuários a escolherem senhas mais seguras.

8.1.1.7.Recuperação de Senhas

O processo de recuperação de senhas será seguro e incluirá autenticação multifatorial para garantir que somente o usuário legítimo possa recuperar o acesso.

8.1.1.8.Proibição de Senhas Repetidas

Não será permitido o uso de senhas repetidas. Cada nova senha deverá ser única, sem reutilização de senhas anteriores.

8.1.1.9.Proibição de Uso de Informações Pessoais

Será proibido o uso de informações pessoais como nomes de familiares, datas comemorativas ou nomes de animais de estimação, para evitar que senhas sejam facilmente adivinhadas ou descobertas.

8.1.1.10. Monitoramento

A equipe de TI realizará auditorias periódicas para garantir que as políticas de senhas e MFA estejam sendo seguidas.

8.2.Ferramenta de senhas

Os gerenciadores de senha são ferramentas essenciais para garantir a segurança das credenciais de acesso aos sistemas e serviços utilizados pelos funcionários. Eles permitem a criação e o armazenamento seguro de senhas, além de garantir que as senhas fortes sejam usadas e que a gestão de acesso seja centralizada, o que facilita a auditoria e o controle. Há vários gerenciadores no mercado, porém, para a FecafTECH, vamos usar o Bitwarden sendo uma solução avançada e intuitiva para proteger identidades digitais e reforçar a segurança online. Ele oferece recursos como:

- Autenticação de dois fatores
- Preenchimento automático de formulários
- Funcionalidade biométrica
- Gerador de senhas
- Encriptação de ponta a ponta dos dados no cofre
- Histórico para ver as palavras-passe anteriores

- Partilha segura de itens do cofre com outros utilizadores Bitwarden

9. RISCOS A LONGO PRAZO DA FALTA DE CONSCIENTIZAÇÃO EM SEGURANÇA CIBERNÉTICA

Muitos ainda consideraram a conscientização da segurança uma questão secundária ou de responsabilidade exclusiva do departamento de TI. No entanto, ignorar a conscientização dos colaboradores em relação às ameaças cibernéticas pode ter consequências desastrosas a longo prazos, a seguir, os cenários que podem ocorrer:

a. **Aumento significativo no numero de incidentes na segurança:** Em vista que o programa não foi eficiente, a falta de conscientização dos colaboradores resultará em mais incidentes de segurança, como o clique em links maliciosos, o uso de senhas fracas e o compartilhamento inadequado de informações confidenciais. Os funcionários tornam alvos fáceis de ataques de phishing, engenharia social e malware, comprometendo a segurança da empresa. Isso resultará em uma exposição constante a riscos de segurança, com incidentes cada vez mais frequentes.
b. **Riscos financeiros:** A violação de dados pode resultar em sérios custos com recuperação de dados, multa por violação de regulamentações de segurança (como GDPR ou LGPD) e o pagamento de resgates em casos de ataques de ransomware. Além disso, o custo de reparar a reputação da empresa após um incidente de segurança pode ser muito alto.
c. **Interrupções nas operações**: Alguns ataques podem levar a interrupções dos sistemas afetando a produtividade dos funcionários e interrompendo as operações diárias da FecafTech.

Esses são alguns dos potenciais cenários que a não implementação de um programa de conscientização e proteção de dados eficaz na FecafTECH resultará. A longo prazo, isso poderá comprometer não apenas a integridade dos dados e do sistema, mas também a reputação e a saúde financeira da empresa.

CONCLUSÃO

Com a implementação deste plano de conscientização em segurança cibernética a FecafTECH terá uma abordagem estruturada para mitigar os riscos associados a incidentes de segurança, especialmente aqueles causados por erros humanos. Com a integração das práticas de segurança no cotidiano dos colaboradores e promovevendo uma cultura organizacional de proteção de dados, a empresa estará significativamente mais preparada para enfrentar as ameaças cibernéticas e proteger seus dados sensíveis.

A conscientização contínua e o treinamento regular são fundamentais para criar uma mentalidade proativa em relação à segurança, garantindo que todos na organização compreendam o papel essencial que desempenham na defesa contra ataques e na preservação da integridade dos sistemas.

Com a implementação deste plano, a FecafTECH não só reduzirá vulnerabilidades, mas também fortalecerá sua reputação no mercado, demonstrando compromisso com a segurança de seus clientes e colaboradores.

REFERÊNCIAS

BISHOP, Matt. **Computer Security: Art and Science**. 2. ed. Boston: Pearson Education, Inc., 2019.

BRASILINE TECNOLOGIA. **Análise Detalhada das Estatísticas e Principais Riscos Corporativos no Relatório Verizon** *DBIR* 2023. Disponível em: https://brasiline.com.br/blog/analise-detalhada-das-estatisticas-e-principais-riscos-corporativos-no-relatorio-verizon-dbir-2023/. Acesso em: 19 dez. 2024.

FOROUZAN, Behrouz *A*. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw-Hill, 2008.

GALVÃO, Michele da Costa (org.). **Fundamentos em segurança da informação**. São Paulo: Pearson, 2015.

MEDEIROS, Luciano Frontino. **Banco de dados: princípios e prática.** 1. ed. Curitiba: Intersaberes, 2013.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Cybersecurity Framework Version** 1.1 [Special Publication 800-161]. 2024. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.ipd.pdf. Acesso em: 19 dez. 2024.

SETZER, W. W.; SILVA, F. S. C. da. **Bancos de dados: aprenda o que são, melhore seu conhecimento, construa os seus**. 1. ed. São Paulo, SP: Blucher, 2005.

SÊMOLA, M. **Gestão da segurança da informação: visão executiva da segurança da informação**. Rio de Janeiro: Elsevier, 2003.

SILVA, Michel Bernardo Fernandes da. **Cibersegurança: uma visão panorâmica sobre a segurança da informação na internet.** Rio de Janeiro: Freitas Bastos, 2023.

STALLINGS, William. **Criptografia e segurança de redes: princípios e práticas**. 6. ed. São Paulo: Pearson, 2014.

TALAGALA, Nishata. **Data as the new oil is not enough: Four principles for avoiding data fires**. Forbes, 2 mar. 2022. Disponível em: https://www.forbes.com/sites/nishatalagala/2022/03/02/data-as-the-new-oil-is-not-enough-four-principles-for-avoiding-data-fires/#:~:text=Generally%20credited%20to%20mathematician%20Clive,it%20cannot%20really%20be%20used. Acesso em: 10 dez. 2024.

ANEXOS

Anexo A – Relatorio do desafio segurança Cibernetica

O vídeo a seguir apresenta um resumo do projeto detalhando os principais conceitos e justificativas técnicas empregados no desafio.

Link do vídeo: [Clique aqui]

Anexo B – Apresentação do desafio de seguranca cibernética

A apresentação em PowerPoint complementa o vídeo e detalha visualmente os aspectos do projeto.

Link da apresentação: [Clique aqui]