Segurança Cibernética para Pequenas e Médias Empresas: Ameaças, Prevenção e Conformidade - Um Estudo Teórico e Prático

Lucas Steisiney Tamanaka Amorim, Jucele França de Alencar Vasconcellos[1]

[1]Faculdade de Computação (FACOM) - Universidade Federal de Mato Grosso do Sul (UFMS)
Campo Grande - Mato Grosso do Sul - Brasil

lucas.tamanaka@ufms.com, jucele.vasconcellos@ufms.br

Abstract. *This article investigates the challenges of cybersecurity in small and medium-sized enterprises (SMEs), with an emphasis on the prevalence of phishing attacks. Two local SMEs were analyzed to assess their cybersecurity practices, including processes, employee compliance with secure protocols, network protection, and response procedures for device loss. The results indicate non-compliance with essential security recommendations, highlighting the need for improvements.*

Resumo. *Este artigo investiga os desafios de segurança cibernética em pequenas e médias empresas (PMEs), com ênfase na prevalência de ataques de phishing. Duas PMEs locais foram analisadas para avaliar suas práticas de segurança cibernética, incluindo processos, conformidade dos colaboradores com protocolos seguros, proteção de rede e procedimentos de resposta para perda de dispositivos. Os resultados indicam não conformidade com recomendações essenciais de segurança, destacando a necessidade de aprimoramentos.*

1. Introdução

A tecnologia da informação é parte fundamental do dia a dia das pessoas e no meio empresarial. Antes, apenas grandes empresas tinham acesso à recursos computacionais, mas hoje a realidade é diferente: 99% das pequenas e médias empresas usam pelo menos uma ferramenta digital em suas operações diárias [Deloitte 2019]. Segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), uma empresa média é aquela que emprega até 250 funcionários enquanto uma pequena tem menos de 50, sendo que esta definição pode variar de país a país. Já no Brasil, existem outras formas de classificar o porte de uma empresa. Este trabalho levará em conta a classificação dada pelo Serviço Brasileiro de Apoio às Micro e Pequenas Empresas (SEBRAE), que considerando o setor de Comércio e Serviços, define: (i) Microempresa: até 9 colaboradores; (ii) Pequena empresa: 10 a 49 colaboradores; (iii) Média empresa: 50 a 99 colaboradores; (iv) Grande Empresa: mais de 100 colaboradores [SEBRAE 2020].

Ao aumentar o uso de tecnologia nas empresas, cresce também a preocupação dos empresários com a segurança cibernética, que pode ser definida: *Segurança Cibernética é a organização e coleção de recursos, processos e estruturas usadas para proteger um ciberespaço e um conjunto de sistemas cibernéticos de ocorrências que desalinhem o*

direito de propriedade de jure com o de facto. [Dan Craigen 2014]. Ou seja, proteger que o verdadeiro dono da informação (*de jure*) tenha as informações roubadas, acessadas ou violadas por um possível invasor (*de facto*).

Em concordância com a primeira definição apresentada, [Mark Merkow 2006] estabelece o tripé da segurança da cibernética em uma companhia:

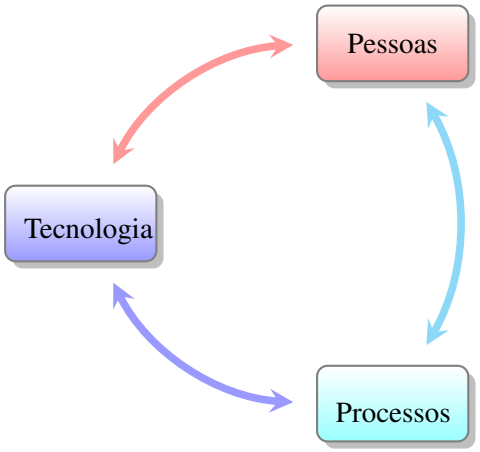

Figura 1. Tripé da Segurança Cibernética. Adaptado de [Mark Merkow 2006]

Dadas as devidas definições, é importante analisar também o grau de preocupação dos dirigentes de companhias em relação à segurança. Um levantamento feito pela seguradora [Allianz 2022] mostra que a preocupação relacionada à a segurança cibernética é a principal no meio empresarial, superando até mesmo a interrupção total de suas atividades e também de desastres naturais.

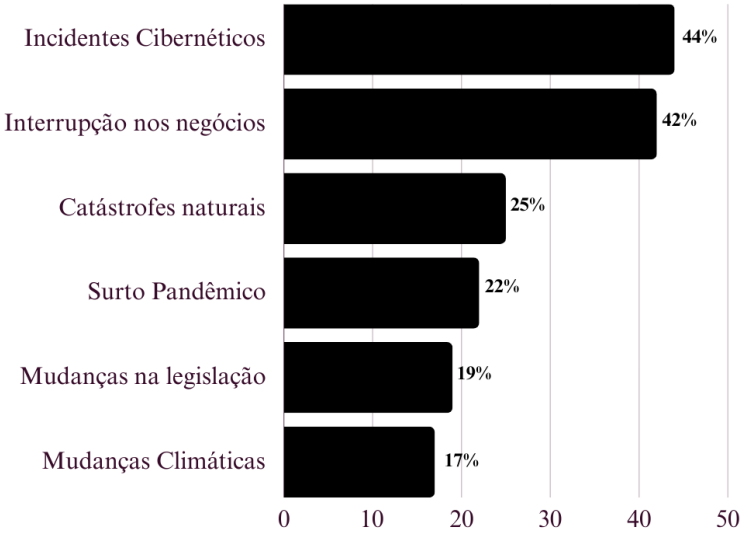

Figura 2. Os mais importantes riscos para negócios em 2022. Adaptado de [Allianz 2022]

O dado mais alarmante é que 43% dos ataques estão centrados em pequenas e médias empresas, sendo que apenas 14% delas tem medidas de defesas eficientes

[Kelly Bissell 2019]. O que traz ainda mais preocupação para estes tipos de negócios não são nem tanto os impactos diretamente causados pela interrupção de serviços trazidos pelo ataque, mas o custo para restabelecer a infraestrutura de tecnologia da informação que por vezes é danificada a ponto de ser irreparável.

Segundo relatório publicado por [Ponemon 2020] os maiores meios de ataque utilizado em pequenos negócios são: *Phishing* / Engenharia Social (57%), Roubo de dispositivos (33%) e Roubo de credenciais (30%).

Este trabalho propõe medidas mínimas, baseadas na literatura e implementações em ambientes reais, que sejam possíveis de implementar diante da realidade de uma micro, pequena ou média empresa, a fim de mitigar os riscos de um ataque cibernético.

2. Referencial Teórico

Esta seção tem como objetivo apresentar os referenciais teóricos que fundamentarão a metodologia e as considerações finais deste trabalho. Inicialmente serão abordados e definidos os tipos de ataques empregados em organizações, juntamente com as formas de prevenção previstas na literatura. Além disso, serão discutidas as métricas utilizadas para mensurar a maturidade da segurança da informação em uma organização, bem como o risco cibernético. Esses referenciais serão empregados como base para a análise do risco cibernético mencionada na introdução.

2.1. Tipos de Ataques e Medidas de Prevenção

No contexto das pequenas e médias empresas, os ataques mais comuns incluem engenharia social, roubo de dispositivos e roubo de credenciais. Embora haja diversos outros tipos de ataques utilizados por criminosos, este trabalho focará apenas nos três mencionados, pois estão diretamente relacionados ao escopo desta pesquisa.

2.1.1. Engenharia Social

No contexto de segurança cibernética, engenharia social é: *o termo usado para descrever o uso de truques psicológicos, que é a manipulação de comportamento muitas vezes através do engano, por criminosos cibernéticos em usuários inocentes para ganhar acesso à informação* [Alan N. Chantler 2008].

Existem várias formas pelas quais os criminosos podem se aproveitar para ganhar acesso às informações. Todas essas formas partem da premissa de ganhar a confiança do usuário trazendo algum fato crível, para então aplicar o golpe. Ainda segundo [Alan N. Chantler 2008], a engenharia social manipula qualquer desejo inato do indivíduo: amizade, romance, ganância ou senso de urgência.

O que faz a engenharia social um dos maiores meios de ataques, conforme já mencionado anteriormente, é que não importa o quão eficazes sejam as defesas implementadas, elas não bastarão caso as pessoas não sejam treinadas, alertadas e capacitadas sobre o assunto.

São alguns dos métodos utilizados na engenharia social:

- **Telefone:** o criminoso liga para a vítima e se apresenta como uma pessoa com algum tipo de autoridade e utiliza técnicas para extrair as informações requeridas;

- **Live:** os indivíduos ganham acesso ao prédio onde está localizado o sistema para obter informação que posteriormente pode ser usada para ganhar acesso ao sistema. *Dumpster Diving* e *Shoulder Surfing* fazem parte desta técnica;
- **Dumpster Diving:** quando criminosos se aproveitam de lixos (papéis, CDs e HDs antigos) para recuperar documentos com informações importantes, tais como registros de funcionários e outros documentos que possam ajudar o ataque de engenharia social;
- **Shoulder Surfing:** quando alguém se aproveita para olhar sobre os ombros de alguém que está digitando alguma senha ou informação importantes no computador;
- **Phishing:** os criminosos enviam e-mails apresentando-se como uma organização legítima (por exemplo, um banco). Uma URL, que direciona para um site fraudulento, é fornecida para a vítima para quem é pedido a confirmação de informações pessoais (senha e usuário, por exemplo). Posteriormente, estas informações podem ser usadas para ganhar acesso à conta da vítima;
- **Pharming:** similar ao *Phishing*, no sentido do usuário acreditar que está informando seus dados pessoais para um site legítimo, quando na verdade está em um site fraudulento que envia os dados para o criminoso, para uso posterior. O *Pharming* interfere na verdade na conversão da URL para IP, intervindo diretamente nos servidores DNS. Assim, quando a vítima digita o nome do site na barra de endereço, automaticamente é redirecionada para um site malicioso.

2.1.2. Roubo ou acesso físico a dispositivos

Como mencionado anteriormente, o roubo de dispositivos é parte expressiva das ameaças sofridas por pequenas organizações. E, na verdade, é algo que grandes organizações que possuem espaços abertos ao público também enfrentam, tais como hospitais, escolas e instituições governamentais. [M. Marshall 2008] mostra que 46% de vazamentos de dados ocorridos no Reino Unido, ocorreram nestes tipos de organizações, onde o público pode ter acesso fácil aos dispositivos.

Mesmo que se consiga proteger as informações das organizações usando ferramentas e mecanismos inteligentes, capazes de repelir ameaças como vírus e outros tipos de ataques mais sofisticados, ter acesso físico aos equipamentos, tais como servidores e *laptops*, pode ser um fator facilitador para que um atacante consiga roubar informações ou mesmo credenciais que lhe concederão acesso ao ambiente como um todo.

Como exemplo, [Ellick M. Chan 2008] descreve a técnica de *BootJack*, onde o atacante força inúmeras reinicializações em um computador. Aproveitando-se das informações residuais existentes na memória principal, mesmo após a reinicialização, o atacante então utiliza um dispositivo USB contendo um *malware*, ganhando acesso privilegiado à funções do Sistema Operacional, tais como sessões de VPN, sessões seguras do navegador de internet e também discos encriptados. Pela maneira que este ataque foi desenhado, ele não deixa traços evidentes para ser detectado por sistemas de proteção, como antivírus.

Em suma, nota-se que o acesso físico, seja ele temporário ou por roubo de dispositivo, representa uma ameaça real a segurança cibernética de uma instituição.

2.1.3. Roubo de Credenciais

O roubo de credenciais pode ser realizado de algumas formas. Uma delas é pelos métodos empregados pela engenharia social, conforme já mostrado anteriormente. Outros métodos mais avançados usados por atacantes, podem utilizar *malwares*, que são programas plantados por alguém com intenções maliciosas para causar efeitos imprevistos ou indesejados [Pfleeger 2015], ou outras vulnerabilidades do Sistema Operacional do computador da vítima.

Um dos métodos usados é o *Keylogging*, que consiste em instalar um software malicioso capaz de capturar o que a vítima está digitando em seu teclado. Dependendo da forma como o software for implementado, torna-se difícil de detectar suas atividades [Desimone 2012].

Outra forma utilizada é a captura dos *hashes* correspondentes à senha da vítima no Sistema Operacional. Uma vez capturado, a *hash* pode ser quebrada por força bruta ou mesmo, através de vulnerabilidades do sistema, o atacante pode usar a própria *hash* para autenticar no sistema. Por exemplo, o *Windows*, por exemplo, usa os protocolos de autenticação *NTLM* e *Kerberos*, que suportam a tecnologia *Single Sing-on* (SSO). Isso significa que uma vez que a senha do usuário é informada, a *hash* correspondente é armazenada em memória, para que das próximas vezes ele não necessite digitar sua senha novamente. Apesar da praticidade, existem algumas ferramentas como a *Metasploit psexec*, que usando-se das *hashes* relacionadas às credenciais armazenadas em *cache*, consegue criar um serviço de forma remota no *Windows* e executar um código malicioso [Desimone 2012].

2.1.4. Medidas de prevenção existentes

Apesar dos avanços tecnológicos no campo da segurança cibernética, incluindo não só novas ferramentas como também novos métodos, o elemento humano é figura central nos objetivos de criminosos. Mesmo que se tenha uma estrutura robusta, como soluções de antivírus e firewall, as empresas precisam levar em conta elementos técnicos e não técnicos para conseguir montar um mecanismo de segurança de multicamadas (ou defesa em profundidade). Existem então, medidas que segundo [Nabie Y. Conteh 2016] podem ser incorporadas a fim de aumentar a defesa contra ataques:

- **Política de segurança:** Uma política de segurança de informação e dados bem escrita, contendo dados técnicos e não técnicos, integrando a segurança ao serviço operacional da empresa.
- **Educação e treinamento:** É de suma importância que os funcionários sejam bem treinados e estejam cientes não somente dos riscos mas em como evitar ser pego em um ataque e o que devem fazer caso notem algo suspeito.
- **Guia de Rede:** As organizações precisam ter uma rede bem segura, contendo uma *whitelist* dos sites que são autorizados dentro de seus domínios, usando a Tradução de Endereços de Rede (*Network Address Translation* - NAT), e desabilitar portas e aplicações que não são mais usadas e portanto, por estarem desatualizadas, oferecem brechas que podem ser usadas em ataque. Além disso, os usuários de rede devem ter tempo de expiração de senha de no máximo 60 dias.

- **Auditoria e *Compliance* (Conformidade):** As empresas precisam ter meios de garantir que suas políticas de segurança estejam sendo aplicadas em todos os níveis. Há necessidade então que controles de detecção sejam implantados, tais como revisão de logs de rede, revalidação de permissões de usuários de funcionários e checagem das configurações das estações de trabalho.
- **Aparatos de segurança:** A rede deve dispor de múltiplas camadas de defesa para proteger os dados e o núcleo da infraestrutura. Estas defesas incluem softwares para Prevenção de Intrusão (IPS), Detecção de Intrusão (IDS) e *firewall* em todos os dispositivos. Redes de Perímetro (DMZ), filtros web e Redes Virtuais Privadas (VPN) devem ser instaladas em todas as interfaces externas.

2.2. Padrões, normas e métricas para segurança da informação

Existem alguns padrões, normas e *frameworks* que se propõem a, de alguma forma, medir o nível de maturidade de uma organização no que tange a segurança cibernética e de dados. Além disso, outros definem níveis com ênfase à governança de TI, que pode ter seu entendimento estendido para abranger também os processos, tecnologias e organização de pessoas inerentes à segurança cibernética.

2.2.1. ABNT NBR ISO/IEC 27001

É uma norma adaptada pela Associação Brasileira de Normas Técnicas (ABNT), baseando-se na original ISO/IEC 27001. Tal norma tem como objetivo ”prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação”[ABNT 2022]. A ABNT estabelece nesta norma, um conjunto de conceitos e processos, que visam guiar a organização a ter políticas e padrões corretos, para assegurar que as informações circulem e sejam mantidas de maneira segura.

Alguns pontos podem ser destacados desta norma:

- **Entender a organização:** Deve-se identificar quem são as partes interessadas, quais os requisitos e quais suas expectativas. Além disso, é importante definir qual o escopo do sistema de gestão da segurança da informação;
- **Liderança:** A alta gestão deve estar comprometida com o sistema de gestão da segurança da informação adotado, de forma a assegurar que os princípios e políticas sejam estabelecidos, cumpridos e que sejam compatíveis com a estratégia da organização. Faz parte também das atribuições dos altos gestores, colaborar com recursos, comunicação, promoção de melhoria contínua e apoio às demais áreas estratégicas, na aplicação das políticas e processos estabelecidos.
- **Ações para abordar riscos e oportunidades:** A organização deve identificar, prevenir e reduzir efeitos de riscos indesejados. Além disso, deve-se elaborar processos dentro do sistema de gestão da segurança de informação para lidar com os riscos e oportunidades, além de tornar possível avaliar a eficácia de tais processos.
- **Mudanças:** As mudanças dentro do sistema de gestão da informação devem ser conduzidas de forma planejada
- **Apoio:** A organização deve fornecer recursos e pessoas necessárias para que o sistema de gestão da segurança da informação não seja prejudicado e possa

operar de maneira eficaz. Além disso, ela deve colaborar com a conscientização e também na comunicação para todas as partes interessadas. Como parte disso, a organização deve criar, manter e atualizar documentação abrangente sobre o sistema de gestão da segurança da informação.

- **Avaliação de desempenho:** a organização deve ser capaz de medir, monitorar, analisar e avaliar o sistema de gestão da segurança da informação. Além disso, deve ser possível auditá-lo. Outro ponto importante, é que a Direção deve constantemente analisar criticamente o desempenho da segurança da informação na organização.
- **Melhoria:** Deve-se estabelecer um processo de melhoria continua para adequação e eficácia do sistema de gestão da segurança da informação

2.2.2. COBIT

O **COBIT**, que significa *Control Objectives for Information and Related Technologies* (Objetivos de Controle para Tecnologia da Informação e Tecnologias Relacionadas, em português), é um framework de governança de TI amplamente reconhecido e utilizado em organizações ao redor do mundo. Ele foi desenvolvido pela ISACA (*Information Systems Audit and Control Association*) e oferece um conjunto de melhores práticas e diretrizes para a gestão e governança de tecnologia da informação.

O COBIT é projetado para ajudar as organizações a alcançar seus objetivos de negócios por meio da eficaz gestão de seus recursos de TI, garantindo a entrega de valor, gerenciamento de riscos e conformidade com regulamentações. Ele fornece um conjunto de processos e controles que auxiliam na tomada de decisões estratégicas, monitoramento e melhoria contínua das operações de TI ([ISACA 2019]).

O *framework* COBIT é composto por cinco princípios-chave:

1. **Fornecer Valor para a as partes interessadas:** Garantir que a TI esteja alinhada com os objetivos de negócios e entregue valor mensurável.
2. **Abordagem holística:** Gerenciar a TI de tal forma que componentes de diferentes tipos possam trabalhar juntos, de forma holística, ou seja: enxergando o todo.
3. **Sistema de governança dinâmico:** Garantir que o sistema de governança possam ser maleáveis, e os impactos das mudanças devem ser considerados.
4. **Governança distinta de gestão:** Deve prever a diferenciação de governança e gestão.
5. **Adaptado às necessidades da organização:** O sistema de governança deve ser adaptado à realidade.
6. **Sistema de governança ponta a ponta:** O sistema de governança deve cobrir a organização de ponta a ponta, considerando não apenas o que a TI faz, mas observando o uso de tecnologia em todas as áreas do negócio.

Derivado do CMM (*Capability Maturity Model*), o COBIT faz uso da medição de capacidade através do modelo de maturidade, para estabelecer os requisitos de governança de TI, monitorar e determinar o nível apropriado de controle e desempenho. Em si, o *framework* foca-se em processos e indicadores para governança de TI, mas pode-se relacionar essas métricas e formas de obtê-las com os processos estabelecidos na Segurança Cibernética de uma organização, a fim de sistematizá-los e medi-los.

2.3. Orientações da Comissão Federal de Comunicações dos Estados Unidos

Os padrões e métricas existentes, feitos por grandes instituições como a ISO, possuem objetivos e metologias que, em sua maioria, não são aplicáveis de maneira intuitiva em pequenas empresas. De fato, grande parte destes documentos de padronização são pagos, o que inviabiliza sua aplicação por conta de restrições orçamentárias.

Contudo, existem órgãos governamentais ao redor do mundo que emitem orientações para que pequenas empresas e instituições possam estar minimamente protegidas de ataques cibernético, bem como vazamento de informações sensíveis por falta de processos de gestão da segurança da informação. A Comissão Federal de Comunicações dos Estados Unidos (FCC, do inglês: *Federal Communications Commission*), é um desses órgãos. Ele, apesar de independente do governo federal, é supervisionado pelo Congresso americano e tem como atribuição a regulação as comunicações no país, efetuadas por rádio, televisão, de forma cabeada, e por satélite.

Em suma, os pontos abordados pela FCC em suas recomendações são [FCC 2012]:

1. **Treinar pessoas em princípios de segurança:** Estabelecer melhores práticas para os colaboradores, como usar senhas fortes e acessar somente sites seguros e confiáveis. Além disso, estabelecer regras para o tratamento de dados dos clientes da empresa;
2. **Proteger a informação, computadores e redes de ataques cibernéticos:** Manter toda a estrutura de tecnologia da empresa atualizada, com softwares originais e com as últimas correções de segurança. Além disso, possuir softwares de antivírus instalados em todos os ativos da empresa;
3. **Prover segurança de *firewall* para a conexão de internet:** Ter um *firewall* funcionando, impedindo que atacantes externos possam ter acesso facilitado à rede e seus ativos;
4. **Criar um plano de ação para dispositivos móveis:** Dispositivos móveis podem ser significantes ofensores para segurança cibernética, especificamente se eles guardam informações importantes e podem acessar a rede corporativa. É importante que os dispositivos sejam protegidos com senhas, tenham seus dados encriptados e possuam aplicativos de proteção instalados. Além disso, deve haver procedimentos estabelecidos em caso de perda ou roubo dos equipamentos (como rastreamento ou limpeza automática de dados);
5. **Possuir rotinas de backup:** É importante que a organização possua cópias de backup dos dados feitas regularmente.
6. **Controlar acesso físico a dispositivos e criar contas individuais para cada colaborador:** Garantir que haja barreiras físicas, impedindo que pessoas desconhecidas possam acessar os dispositivos sem que um colaborador veja. Além disso, é necessário que cada colaborador tenha seu login e senha individuais e únicos para os dispositivos que acessam, dessa forma, garantindo assim controle mais refinado dos acessos;
7. **Manter as redes de *Wi-Fi* seguras:** Usar senhas fortes e protocolos de encriptação mais modernos e seguros, para garantir que invasores não se aproveitem de brechas de segurança. Além disso, ocultar a rede, pode ser uma configuração que ajude a dificultar ataques;

8. **Aplicar melhores práticas para sistemas de pagamento:** É importante certificar que os computadores onde os pagamentos são processados via *Internet Banking* estejam com os *plugins* de segurança dos bancos válidos e seguros. Além disso, recomenda-se isolar o computador que faz tais operações, para que o mesmo não seja usado para navegação em páginas de *web* comuns e leitura de e-mails;
9. **Limitar o acesso à dados e permissão de administrador nas estações de trabalho:** É importante regular o acesso aos dados mais importantes apenas aos colaboradores autorizados. Além disso, é importante que os colaboradores sejam impedidos de instalar **softwares** por conta própria em suas estações de trabalho. Para regular isso, é necessário então que existam níveis de acessos dentro da arquitetura proposta para o ambiente da organização;
10. **Senhas e autenticação:** É necessário que os colaboradores usem senhas seguras e as troquem a cada três meses. Além disso, recomenda-se a utilização de autenticação de múltiplo fator, fortalecendo ainda mais a segurança do ambiente.

3. Trabalhos Relacionados

Dentro da temática pesquisa, é certo que pode-se destacar o *Phishing* como uma das principais ameaças, não só no meio em que este trabalho dedica-se a pesquisar, mas como um todo.

O artigo *The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection* [Hakim et al. 2021] levanto em conta um número de voluntários selecionados, tenta pontuar e-mails com relação ao seu grau de suspeita de ser uma mensagem de *Phishing*. Um ponto de originalidade importante deste estudo é que, além de e-mails que simulavam ataques, foram incluídos e-mails reais, coletados pelos pesquisadores. Desta forma foi possível não somente medir o que a teoria cognitiva diz sobre o comportamento de uma vítima, mas testar a efetividade dos ataques lançados por criminosos. A pesquisa conclui que 62% dos e-mails foram classificados corretamente como *Phishing*. Apesar de ser a maior parte, é ainda uma pontuação muito aquém do ideal.

Ademais, o estudo também mostra que e-mails bem projetados por criminosos e lançados em ataques reais, tiveram o índice de suspeição menor do que a média geral. Ou seja, em um cenário real, os voluntários teriam mais chances de cair em um golpe, mostrando que as estratégias usadas pelos atacantes estão certamente tendo o efeito esperado.

4. Metodologia

Nesta sessão será apresentada a metodologia adotada para a realização da pesquisa. Ela tem como objetivo analisar a situação atual de duas empresas, identificar suas vulnerabilidades em relação à proteção cibernética e propor medidas de segurança eficazes. Além disso, foi realizado um teste de phishing falso, seguido por um treinamento, seguindo as práticas levantadas no referencial teórico

4.1. Design da Pesquisa

A pesquisa foi conduzida por meio de um estudo de caso em duas pequenas empresas que atuam no setor imobiliário. A escolha do estudo de caso permite uma análise aprofundada da situação da empresa em relação à segurança da informação, permitindo uma compreensão abrangente das práticas de proteção cibernética adotadas.

4.1.1. Análise da Situação Atual

Para compreender a situação atual da empresa em termos de segurança da informação, foram coletadas informações por meio de um formulários, com perguntas simples pois ambas as empresas não possuem setor específico de tecnologia da informação para guiar questões técnicas aprofundadas. As perguntas seguiram os pontos de verificação propostos pela FCC, mostradas no item 2.3. Optou-se por usar, em sua maioria, questões fechadas de múltipla escolha ou dicotômicas [Marconi 2017]. Dado o ambiente de ambas as empresas, segundo [Mattar 2014], este seria o mais adequado pois são mais fáceis de assimilar e apresentam pouca possibilidade de erro, apesar de ficarem suscetíveis a erros sistemáticos que podem ocorrer ao se elaborar a pergunta.

4.1.2. Teste de Phishing

Por ser um dos maiores ofensores à segurança de pequenas e médias empresas, optou-se por se realizar um teste de *phishing* falso para avaliar a suscetibilidade dos funcionários a ataques de engenharia social.

4.1.2.1. Ataque via e-mail

O ataque de *phishing* foi aplicado pela ferramenta *open-source GoPhish*. Esta ferramenta *open source* é própria para ataques simulados e provê uma quantidade relevante de recursos que podem ser usados. Foram seguidos os seguintes passos, da configuração ao envio do ataque:

1. **Instalação:** A aplicação foi instalada em um servidor no provedor de nuvem AWS (*Amazon Web Services*). Desta forma, permitiu a comunicação entre seus sensores de monitoramento de atividades (abertura de e-mail e clique em *links*). Após a instalação, foram realizadas as devidas configurações de rede para tornar a interface de gerenciamento acessível por um navegador *Web*.
2. **Configuração:** Após instalado, foi necessário realizar a configuração da aplicação para que ela conseguisse realizar o envio de e-mails através do protocolo SMPT (*Simple Mail Transfer Protocol*) e também monitorar as visitas aos sites e abertura de e-mails. Além da configuração da forma do envio, catalogaram-se os colaboradores que foram alvo da simulação;
3. **Elaboração do e-mail:** Parte fundamental da simulação. Para tanto, foram usados todos os conceitos teóricos apresentados no item 2.1.1., conforme [Alan N. Chantler 2008], tentando ganhar a confiança do usuário e também manipulando algum desejo inato do indivíduo, como o senso de urgência. Para isso, a mensagem eletrônica criada (Figura 3) solicita que o colaborador altere sua senha de sistema, para um padrão mais seguro, disponibilizando um *link* para que isso seja feito, mas que na realidade direciona o colaborador a uma página falsa, clonada a partir da original acessada como painel administrativo. Caso ele digite seu login e senha para entrar, será possível capturar essas informações do formulário HTML da página. Para ganhar a confiança do colaborador, na construção visual do e-mail utilizou-se a marca da empresa bem como a paleta de cores de sua identidade visual.

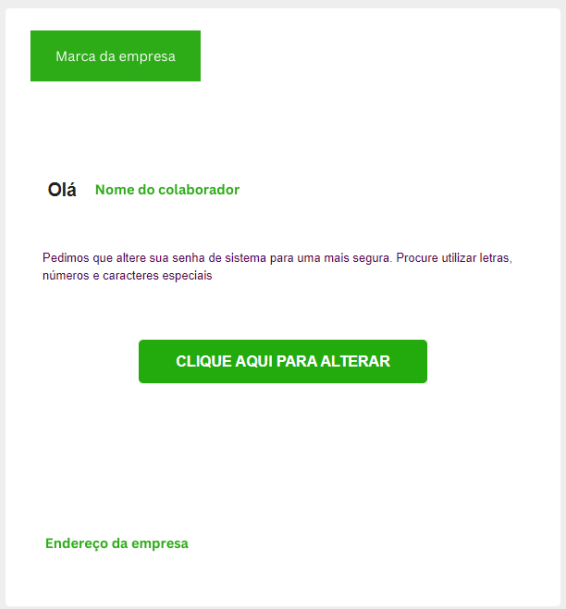

Figura 3. *Mockup* do e-mail a ser enviado

4. **Envio e monitoração:** Com o e-mail configurado e todas as configurações realizadas, realizou-se o envio da campanha para todos os colaboradores. A partir disso, o sistema monitorou por 3 dias consecutivos se: (i) o e-mail chegou corretamente à caixa de entrada; (ii) o colaborador abriu o e-mail, podendo esta função ser bloqueada por alguns provedores por questões de segurança; (iii) o colaborador clicou no *link* disponibilizado; (iv) o colaborador reportou o e-mail como *SPAM*.

4.1.2.2. Ataque via *Whatsapp*

Segundo pesquisa realizada em 2022, o Brasil possui 165 milhões de usuários do aplicativo de mensagens instantâneas *WhatsApp*, sendo que deste total, 79% utilizam a solução para conversar com empresas e comprar seus produtos [Opinion-Box 2023]. Além disso, a empresa de soluções de segurança russa *Kaspersky*, detectou cerca de 76 mil tentativas de fraude em 2022, representando 82,71% dos links bloqueados por suas aplicações de proteção de dispositivos, conforme aponta o relatório emitido no mesmo ano [Kaspersky 2022]. Isso coloca o Brasil como país que mais sofre ataques de *phishing* através deste aplicativo de comunicação no mundo.

Por isso, torna-se relevante testar o comportamento dos colaboradores de ambas as empresas, frente à uma tentativa de golpe via WhatsApp. Para isso, foi utilizado um número novo adquirido de alguma operadora, com uma conta nova conta criada no aplicativo em nome de uma empresa fictícia de serviços de RH. Na mensagem enviada aos colaboradores enviou-se um *link*, direcionado a um formulário, que requisitará que a pessoa informe dados sensíveis como nome, CPF e endereço residencial. É importante lembrar que um atacante real poderia usar este *link*, direcionando para um repositório que faria o *download* de algum arquivo malicioso, sendo que o prejuízo fosse causado não só por informar os dados mas também pelos efeitos de tal programa indesejado. Respeitando o

que a literatura aborta, a simulação tenta ganhar a confiança do usuário, de forma a induzir que ele clique no endereço e informe os dados solicitados.

4.1.3. Intervenção e Treinamento

Com base nos resultados da análise da situação atual e do teste de *phishing*, foram propostas medidas de segurança adequadas para a empresa. Isso inclui a implementação de soluções técnicas e ações de conscientização. Um treinamento de segurança da informação será indicado aos colaboradores, abordando práticas seguras, identificação de ameaças e procedimentos de resposta a incidentes.

4.1.4. Análise dos Dados

Os dados coletados durante a pesquisa foram analisados qualitativa e quantitativamente. A análise qualitativa envolve a interpretação das respostas do formulário e a avaliação da eficácia das medidas de segurança propostas. A análise quantitativa inclui o cálculo das taxas de interação nos testes de *phishing*.

4.1.5. Limitações

É importante destacar que a pesquisa se baseia em um estudo de caso único, o que limita a generalização dos resultados. Além disso, a eficácia das medidas de segurança pode ser influenciada por fatores externos não controlados neste estudo.

5. Resultados e Análise

Neste tópico serão abordados os resultados e análise do formulário enviado aos proprietários das empresas estudas e também os resultados dos testes de *phishing* aplicados nos colaboradores.

5.1. Resultado dos formulários

Conforme exposto na metodologia, ambas as empresas não tem uma equipe específica responsável pela tecnologia da informação. Todos os serviços são prestados esporadicamente por terceiros e, portanto, não há processos definidos no tocante a esta área. Diante disso, os resultados aqui exibidos podem ser imprecisos e não representar a realidade em sua totalidade. A empresa A é enquadrada como pequena empresa pela classificação do SEBRAE, possuindo 20 colaboradores. Já a empresa B, é classificada como microempresa, tendo 9 pessoas em seu quadro funcional. No Anexo I é possível encontrar a tabela com todas as respostas.

5.2. Análise das respostas dos formulários

Conforme foi suposto, nenhuma das empresas possui processos implementados. Tampouco, cumprem os requisitos mínimos propostos pelas FCC. Ao analisar de forma mais aprofundada, ambas estão suscetíveis a ataques relacionados a vulnerabilidades dos sistemas operacionais e demais aplicações.

A empresa B não possui nenhuma forma de proteção à rede e também não possui proteções físicas para que os computadores não sejam acessados por pessoas desconhecidas. Além disso, o sistema principal da empresa não exige o uso de senhas seguras, nem troca periódica das senhas. Todos estes fatores poderiam ocasionar vazamento dos dados dos clientes ou roubo das credenciais administrativas, dando poderes ao invasor de modificar dados importantes, rastrear atividades financeiras e causar outros prejuízos à operação do negócio. Contudo, um fator que pode ser benéfico, é que toda a infraestrutura relacionada aos sistemas que são utilizados está em nuvem e é administrado por um terceiro. Supondo que ele siga as melhores práticas da segurança cibernética, isso daria uma camada de proteção à empresa B.

Já a empresa A, possui parte de sua estrutura de servidores dentro na nuvem e outra parte alocada internamente. Por não ter um departamento dedicado à tecnologia da informação, nem rotinas estruturadas de atualizações e verificação de conformidade, os sistemas da empresa A podem ser alvo de atacantes.

Contudo é interessante notar que nenhuma das empresas teve problemas com ataques ou perda de dados. Pode-se supor que o cenário observado na média mundial, de alto índice de incidência de ataques à pequenos e médios negócios ainda não é uma realidade na cidade de Campo Grande. Contudo, pelo escopo da pesquisa, não é possível chegar a uma conclusão.

5.3. Resultado e análise da simulação de ataque de *phishing* via *WhatsApp*

Foram levantados os contatos telefônicos de todos os colaboradores da empresa que usam computadores ou celulares em seu dia a dia de trabalho. Na empresa A, 19 contatos foram informados pelo proprietários e na B, 5. Em posse destes contatos, primeiramente fora enviada a mensagem via aplicativo de comunicação instantânea *WhatsApp* para 5 colaboradores da empresa A. No momento do envio da sexta mensagem, o aplicativo baniu o número que estava sendo.

Além disso, o proprietário da empresa alertou que a simulação causou a movimentação dos colaboradores que receberam a mensagem. Estes desconfiaram rapidamente da mensagem, bloqueando o contato, e reportaram à chefia. Dois fatores podem ter contribuído para isso: (i) as mensagens foram enviadas em um curto espaço de tempo para colaboradores que estavam em um mesmo ambiente, possibilitando que se comunicassem e discutissem a respeito dela, aumentando suas suspeitas. Ou seja, neste caso, a mensagem falhou em conquistar a confiança do colaborador, mesmo que apelasse para outros sentidos dele como o senso de urgência; (ii) segundo o proprietário, algumas semanas antes do teste, vários colaboradores haviam caído em golpes solicitando transferências bancárias via *WhatsApp*. Isso pode ter aguçado a percepção das pessoas, tornando-as mesmo que temporariamente, mais críticas às mensagens que são recebidas.

Como o número adquirido fora banido do *WhatsApp*, optou-se por não realizar esta simulação na empresa B. Além disso, outro fator que levou a esta decisão, foi para não aumentar a desconfiança dos colaboradores antes da simulação via e-mail, preservando os resultados de tal teste.

5.4. Resultado e análise da simulação de ataque de *phishing* via *e-mail*

Para a simulação via e-mail, a empresa A informou 9 e-mails e a B um total de 5. Após realizar toda a configuração da ferramenta *Gophish*, conforme descrito na metodologia, foi realizado o envio das mensagens eletrônicas. Além disso, acionaram-se os sensores da ferramenta para monitoramento de abertura de mensagens e clique nos links.

Em ambas as empresas não foi possível detectar se os colaboradores abriram os e-mails. Conforme fora previsto, pode haver bloqueio no envio destas informações por parte do provedor de e-mail da empresa. Apesar da ferramenta não ter registrado a abertura, o proprietário da empresa A novamente foi alertado por seus colaboradores a respeito de uma mensagem suspeita. Três colaboradores reportaram que receberam uma mensagem que nunca haviam recebido, solicitando a troca de senha do sistema e decidiram não clicar no *link*, optando então por excluir a mensagem de sua caixa de entrada. Já na empresa B não houve nenhum reporte ao proprietário.

Isso pode indicar que os colaborares da empresa A: (i) estão mais atentos quanto à golpes via mensagens eletrônicas; (ii) foram influenciados pelo teste anterior que aumentou sua percepção à golpes.

Contudo, em cada uma das empresas, um colaborador clicou no *link*, entrou na página *web* clonada criada, e informou suas credenciais. Na empresa A, a pessoa que clicou possui acesso ao módulo de sistema financeiro. Caso este fosse um ataque real, suas credenciais teriam elevação suficiente para dar ao atacante acesso aos registros de pagamento e informações bancárias da empresa e clientes. Isso seria suficiente para muni-lo de dados que possibilitariam aplicar golpes de boletos falsos, por exemplo, enviando um boleto forjado direcionado à outra conta. Já na empresa B, o colaborador não possui acesso tão elevado quanto o colaborador da empresa A, mas tem acesso à dados pessoais de clientes e também dos imóveis disponibilizados para aluguel e seus proprietários. Isso poderia dar ao atacante alguma vantagem competitiva, caso este ataque fosse encomendado por uma empresa concorrente, supondo um caso de espionagem industrial.

Vale lembrar, conforme fora feito anteriormente na metodologia, que o *link* enviado para propósitos de simulação redirecionava apenas para um site falso com objetivo de captura de informações. Em uma situação real, o atacante poderia optar por configurar a página para descarregar um arquivo malicioso na máquina da vítima, que por não possuir as proteções adequadas, estaria vulnerável a ataques mais complexos e danosos ao ambiente computacional corporativo, como um *ransomware* que poderia criptografar todos os arquivos da empresa.

5.5. Treinamento e acompanhamento pós simulação

Após a simulação, ambos os proprietários foram orientados a respeito das vulnerabilidades em suas empresas bem como do risco e impacto que um ataque como o simulado poderia causar. Com relação às vulnerabilidades, os proprietários foram orientados a: (i) instaurar processos de atualização dos computadores e sistemas de forma periódica, deixando-os seguros quanto à falhas de segurança; (ii) reforçar soluções de proteção como *firewall* e *antivírus* para todo os computadores; (iii) incentivar o uso de senhas seguras (em computadores e dispositivos móveis) e criar barreiras de proteção para que pessoas não autorizadas sejam impedidas de acessar os computadores; (iv) treinar constantemente os colaboradores; (v) manter as rotinas de backup ativas.

Com relação ao treinamento, fora elaborada e confeccionada uma aula *online* simples e rápida, definindo os conceitos de segurança, informando os principais métodos de ataque e como se proteger. O material pode ser acessado pelo *link*: `https://link.edapp.com/ObJigdGFbEb`.

6. Trabalhos futuros

Embora esta pesquisa tenha contribuído significativamente para a compreensão da segurança cibernética e do estado atual das duas empresas estudadas, há diversas oportunidades para estudos futuros e aprimoramentos. Uma abordagem promissora seria ampliar a amostra de empresas na cidade, visando obter uma quantidade mais abrangente de dados que permita uma visão holística da segurança da informação em Campo Grande. Este enfoque proporcionaria um panorama mais completo e representativo.

Adicionalmente, ao incluir mais empresas na análise, seria possível investigar mais profundamente o comportamento dos colaboradores diante de ataques simulados de phishing. Esse aspecto, muitas vezes negligenciado, é crucial para a eficácia das estratégias de segurança cibernética, e um estudo mais amplo poderia fornecer ideias valiosas sobre a conscientização e preparo dos funcionários.

Outro ponto de relevância seria a formulação e implementação de processos específicos nas empresas estudadas, seguida por um acompanhamento ao longo de um período determinado. Essa abordagem permitiria avaliar a eficácia das sugestões propostas não apenas na proteção do ambiente computacional, mas também no dia a dia operacional das empresas. Esse monitoramento contínuo seria fundamental para entender como as medidas de segurança impactam diretamente as práticas diárias e contribuem para a resiliência operacional das organizações.

7. Conclusão

Em um cenário empresarial cada vez mais digitalizado, a segurança cibernética emerge como um fator determinante para a integridade e continuidade operacional das Pequenas e Médias Empresas. Este trabalho procurou explorar e compreender os desafios enfrentados por esse segmento específico, identificando os principais conceitos e ataques que impactam diretamente a segurança cibernética dessas organizações.

Ao elencar os ataques mais frequentes, destacamos o *phishing* como uma ameaça particularmente grave para as empresas. A escolha de conduzir uma investigação em duas empresas locais permitiu uma análise da postura de segurança cibernética, abrangendo áreas cruciais, como a existência de processos relacionados à área, o uso de senhas seguras por parte dos colaboradores, a proteção da rede e procedimentos definidos para a perda de dispositivos.

Os resultados obtidos a partir da simulação de teste de *phishing* revelaram uma vulnerabilidade preocupante: em ambas as empresas, ao menos um colaborador clicou no link enviado, evidenciando a urgência de aprimorar a conscientização e treinamento em segurança cibernética. Além disso, os dados levantados indicaram que as empresas não estavam aderindo ao mínimo das recomendações de segurança, destacando a necessidade de uma abordagem mais proativa e eficaz na implementação de medidas de proteção.

Diante dessas constatações, é imperativo que as empresas reconheçam a importância estratégica da segurança cibernética e adotem medidas robustas para mitigar

os riscos associados. Recomenda-se a implementação de programas de conscientização, treinamentos regulares para os colaboradores, adoção de políticas de segurança claras e a utilização de tecnologias de proteção avançadas.

A segurança cibernética nas Pequenas e Médias Empresas não é apenas uma necessidade, mas uma exigência incontornável para garantir a resiliência e o sucesso contínuo dessas organizações em um ambiente digital desafiador.

Referências

ABNT (2022). *ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos*. Associação Brasileira de Normas Técnicas, Rio de Janeiro, RJ, Brasil.

Alan N. Chantler, R. G. B. (2008). Social engineering and crime prevention in cyberspace. https://www.researchgate.net/publication/27468302_Social_Engineering_and_Crime_Prevention_in_Cyberspace, visitado em 27/05/2023.

Allianz (2022). Allianz risk barometer. https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, visitado em 22/05/2023.

Dan Craigen, Nadia Diakun-Thibault, R. P. (2014). Defining cybersecurity. https://www.timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf, visitado em 10/09/2023.

Deloitte (2019). The performance of small and medium sized businesses in a digital world. https://www2.deloitte.com/content/dam/Deloitte/es/Documents/Consultoria/The-performance-of-SMBs-in-digital-world.pdf, visitado em 22/05/2023.

Desimone, J. (2012). Windows credential theft: Methods and mitigations. https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1628&context=theses, visitado em 11/05/2023.

Ellick M. Chan, Jeffrey C. Carlyle, F. M. D. R. F. R. H. C. (2008). Bootjacker: compromising computers using forced restarts. *CCS '08: Proceedings of the 15th ACM conference on Computer and communications security*, pages 555–564.

FCC (2012). Cyber security tips for small business. https://docs.fcc.gov/public/attachments/DOC-306595A1.pdf, visitado em 08/11/2023.

Hakim, Z. M., Ebner, N. C., Oliveira, D. S., Getz, S. J., Levin, B. E., Lin, T., Lloyd, K., Lai, V. T., Grilli, M. D., and Wilson, R. C. (2021). The phishing email suspicion test (pest): A lab-based task for evaluating the cognitive mechanisms of phishing detection. *Behavior Research Methods*, 53(3):1342–1352. https://doi.org/10.3758/s13428-020-01495-0, visitado em 02/12/2023.

ISACA (2019). *COBIT 2019 Framework: Introduction and Methodology*. ISACA. https://www.isaca.org/COBIT/Pages/Framework-Introduction-and-Methodology.aspx, visitado em 08/09/2023.

Kaspersky (2022). El spam y el phishing en 2022. https://securelist.lat/spam-phishing-scam-report-2022/97582/, visitado em 19/09/2023.

Kelly Bissell, Ryan Lassalle, P. D. C. (2019). Ninth annual cost of cybercrime study. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study, visitado em 22/05/2023.

M. Marshall, M. Martindale, R. L. D. (2008). Data loss barometer. *KPMG UK*.

Marconi, M. d. A. (2017). *Fundamentos de metodologia científica*. Atlas.

Mark Merkow, J. B. (2006). *Information Security Principles and Practices*.

Mattar, F. N. (2014). *Pesquisa de marketing : metodologia, planejamento, execução e análise*. Elsevier.

Nabie Y. Conteh, P. J. S. (2016). Cybersecurity:risks, vulnerabilities and countermeasures to prevent social engineering attacks. https://bit.ly/3ugWLfA, visitado em 17/06/2023.

Opinion-Box (2023). Whatsapp no brasil. https://blog.opinionbox.com/pesquisa-whatsapp-no-brasil/, visitado em 19/09/2023.

Pfleeger, C. (2015). *Security in Computing, Fifth Edition*. Prentice Hall.

Ponemon (2020). Cybersecurity in the remote work era: A global risk report. https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf, visitado em 20/08/2022.

SEBRAE (2020). Anuário do trabalho nos pequenos negócios - 2018. https://www.dieese.org.br/anuario/2018/anuarioPequenoNegocio2018/index.html?page=4, visitado em 25/09/2023.

Anexo I

	Empresa A	**Empresa B**
Quantos funcionários usam o computador	12	5
Os dados da empresa são hospedados	Parte em estrutura interna, parte na nuvem	Nuvem
Quais ferramentas de comunicação são utilizadas	E-mail, telefone e WhatsApp	E-mail, telefone e WhatsApp
Os funcionários já realizaram treinamento a respeito da segurança da informação / cibernética	Nunca	Nunca
Existe uma rotina (automática ou manual) para verificar se os computadores da empresa estão atualizados e protegidos	Não	Não
A empresa possui firewall e/ou outras formas de proteção da rede	Sim	Não
Os colaboradores são obrigados a protegerem seus dispositivos móveis com senhas, para dificultar a perda e vazamento de dados, seja por roubo ou extravio?	Não	Não
Existe rotina de backup de dados	Apenas de informações mais importantes	Apenas de informações mais importantes
A rede Wi-Fi da empresa é protegida com uma senha forte	Não	Não
Os dispositivos usados para pagamentos são usados apenas para este propósito	Não	Não
Existem proteção por senha nos computadores e barreiras físicas para protegê-los de acessos de desconhecidos	Sim	Não
Existem maneiras de impedir que os colaboradores tenham acesso a todos os dados da empresa	Sim	Sim
Os funcionários precisam usar senhas fortes em seus acessos e são forçados a trocá-las a cada 3 meses?	Sim	Não
A empresa já sofreu algum tipo de ataque cibernético	Não	Não
Já houve roubo ou vazamento de informações sensíveis dos clientes	Não	Não