SEMANA ACADÊMICA
REVISTA CIENTÍFICA
ISSN 2236-6717

SEGURANÇA CIBERNÉTICA- ESTUDO DAS TÉCNICAS DE ATAQUES CIBERNÉTICOS (PHISHING, RANSMWARE, DDOS) DE ENGENHARIA SOCIAL E MEDIDAS DE PREVENÇÃO

Jhonatan Rodrigues Guzella Dias[1]
https://orcid.org/0009-0007-2536-6411
Renata Mirella Farina[2]
https://orcid.org/0000-0001-9602-5293
Fabiana Florian[3]
https://orcid.org/0000-0002-9341-0417

RESUMO
Ataques cibernéticos é um tema crucial na área de segurança da informação dada a crescente sofisticação e diversidade de ameaças enfrentadas por organizações e usuários individuais. Este trabalho tem o objetivo de estudar diferentes técnicas de ataques cibernéticos, incluindo phishing, ransomware e ataques de negação de serviço (DDoS). O estudo visa compreender como são executados esses ataques, identificar os vetores de ataque e analisar os danos causados às vítimas. Foi realizado pesquisa bibliográfica, qualitativa. Conclui-se que a partir o estudo das técnicas de ataques cibernéticos (*phishing, ransomware e DDoS*), continua sendo um desafio complexo e em constante evolução. O desenvolvimento de programas educacionais e iniciativas de conscientização são fundamentais para prevenção desses ataques bem como a responsabilidade legal e a ética ao proteger os sistemas de informação.

Palavras-chave
LGPD; Phishing; Segurança cibernética; Ameaças.

Submetido em: 29/05/2024 – **Aprovado em**: 05/07/2024 – **Publicado em**: 05/07/2024

1 Discente do curso de Engenharia da Computação da Universidade de Araraquara-SP, ORCID Id: 0009-0007-2536-6411.
2 Administradora, Analista de Sistemas, docente dos cursos de Ciências Administrativas nos cursos de Administração, Computação, Produção e Sistemas de Informação da Universidade de Araraquara-SP, ORCID Id: 0000-0001-9602-5293.
3 Economista, Bacharel em Direito, Docente do departamento de Ciências Administrativas nos cursos de Elétrica, Civil, Computação, Sistemas de Informação e Agronomia da Universidade de Araraquara-SP, ORCID Id: 0000-0002-9341-0417.

http://dx.doi.org/10.35265/2236-6717-248-13011
FORTALEZA-CE. EDIÇÃO 248. V.12. ANO 2024.

CYBER SECURITY - STUDY OF CYBER ATTACK TECHNIQUES (PHISHING, RANSMWARE, DDOS) AND THE ROLE OF PRIVACY AND DATA PROTECTION LAWS

ABSTRACT
Cyberattacks are a crucial topic in the area of information security given the increasing sophistication and diversity of threats faced by organizations and individual users. This work aims to study different cyber attack techniques, including phishing, ransomware and denial of service attacks (DDoS). The study aims to understand how these attacks are carried out, identify attack vectors and analyze the damage caused to victims. Qualitative bibliographical research was carried out. It is concluded that from the study of cyber attack techniques (phishing, ransomware and DDoS), it continues to be a complex and constantly evolving challenge. The development of educational programs and awareness initiatives are fundamental to preventing these attacks as well as legal responsibility and ethics when protecting information systems.

Keywords
Cybersecurity. LGPD. Phishing. Threats.

1 INTRODUÇÃO

Na era digital a segurança cibernética emerge como um pilar fundamental para garantir a integridade, a confidencialidade e a disponibilidade das informações. Para Schneier [s/d] in Lopes (2015) "A segurança é um processo, não um produto." A proteção contra ameaças cibernéticas requer uma abordagem contínua e dinâmica, uma vez que os adversários digitais estão em constante evolução, buscando explorar vulnerabilidades e fragilidades em sistemas e redes. Se torna necessário mitigar essas ameaças, não apenas para proteger os ativos digitais das organizações, mas também para salvaguardar a privacidade e a segurança dos indivíduos em um mundo cada vez mais interconectado e dependente da tecnologia.

A análise de técnicas de ataques cibernéticos abrange uma ampla gama de ameaças, desde os ataques mais simples, como *Phishing,* até os mais devastadores, como *Ransomware* e ataques de negação de serviço (DDoS). Cada uma dessas técnicas representa uma abordagem única utilizada por invasores para comprometer sistemas, roubar informações confidenciais e interromper operações críticas.

Este trabalho tem o objetivo de estudar diferentes técnicas de ataques cibernéticos *(phishing, ransomware, DDoS),* examinando como são executados esses ataques, identificar os vetores de ataques e analisar os danos causados as vítimas. Dessa forma identificar não apenas as vulnerabilidades exploradas por esses ataques, mas também as melhores práticas e medidas de segurança que podem ser implementadas para mitigar seus efeitos maléficos.

Espera-se com este estudo adquirir insights que permitirá projetar e implementar soluções de segurança eficazes, contribuindo para a construção de um ambiente digital mais seguro e resiliente.

Foi realizada pesquisa bibliográfica, qualitativa com foco em ataques cibernéticos, aspectos legais e a ética em segurança cibernética.

2 BREVE CARACTERIZAÇÃO DOS ATAQUES CIBERNÉTICOS

Os ataques cibernéticos são realizados por indivíduos ou organizações com intenções criminosas, políticas ou pessoais de destruir ou obter acesso a informações confidenciais.

O objetivo de um ataque cibernético é causar danos ou obter controle ou acesso a documentos e sistemas cruciais em uma rede de computadores pessoais ou comerciais.

Esta seção apresenta a relação da Teoria econômica com a segurança da informação bem como as técnicas de ataques cibernéticos (*Phishing,* Ataques de Negação de Serviço (DDoS), *Ransomware).*

2.1 Relação da Teoria econômica com a segurança da informação

Anderson (2001) in (CORTEZ; KUBOTA, 2013) foi o primeiro a ilustrar como a teoria econômica se relaciona com a questão da segurança da informação. O autor defende as externalidades de rede, as barreiras à entrada, o fato de as grandes empresas adotarem suas estratégias baseadas no valor, em vez de no custo.

A falta de incentivos econômicos é a fonte de uma grande parte dos problemas de segurança da informação (VARIAN, 2004) in (CORTEZ; KUBOTA, 2013). O autor sustenta que a responsabilidade é ambivalente. Um exemplo são os ataques *Distributed Denial of Service* (DDOS), que ocorreram em 2000 quando hackers invadiram algumas redes desprotegidas de universidades norte-americanas e usaram suas estruturas para enviar ataques a vários sítios eletrônicos, incluindo o Yahoo.

As universidades poderiam ter incentivos para proteger a sua rede se houvesse responsabilização (*liability).* Os custos de ataques DDOS devem ser devidos aos operadores de rede, pois eles têm a capacidade de identificar melhor que setor está mais preparado para mitigar os riscos. (VARIAN, 2004) in (CORTEZ; KUBOTA, 2013).

Anderson (1994) in (CORTEZ; KUBOTA, 2013) aborda a questão das responsabilidades, demonstrando como os padrões de fraude em contas bancárias estão relacionados a esse fenômeno. O autor compara casos de fraude na Grã-Bretanha, na Noruega, na Holanda e nos Estados Unidos. Nos países europeus o ónus da prova estava sobre os clientes e nos EUA, sobre os bancos.

Os bancos na Europa não são incentivados a melhorar seus sistemas de segurança, o que resultou na proliferação da fraude. Nos Estados Unidos, os incentivos eram totalmente o contrário e os bancos tiveram um número significativamente menor de fraudes cometidas.

Cremonini e Nizovtsev (2006) in (CORTEZ; KUBOTA, 2013) examinam o comportamento dos atacantes em vários cenários de informação. Num primeiro cenário, os atacantes obtêm informações detalhadas sobre as características de segurança dos alvos. Num segundo cenário, a analise é feita sob hipótese de informação assimétrica. Os resultados do modelo mostram que quando os atacantes identificam o nível de segurança de seus alvos e alternam entre vários alvos, o efeito de uma medida de segurança específica tem maior impacto. Qualquer melhoria na segurança tem dois efeitos na quantidade de incidentes.

Além disso, os autores demonstram que sistemas com mais proteção têm incentivos mais fortes para revelar suas características de segurança para os atacantes do que sistemas com baixa proteção.

2.2 Tecnicas de Ataques Ciberneticos (Phishing, Ataques de Negação de Serviço (DDoS), Ransomware)

Os ataques de phishing são uma forma de engenharia social que visa enganar os usuários para que divulguem informações confidenciais, como credenciais de login, detalhes financeiros e outras informações pessoais. MALWAREBYTES [s/d]. Existem várias técnicas e métodos que os invasores utilizam para conduzir esses ataques tais como: blind phishing e clone phishing.

E-mails de phishing são uma das maneiras mais comuns de conduzir esses ataques. Os invasores enviam e-mails fraudulentos que se fazem passar por comunicações legítimas de empresas, instituições financeiras ou indivíduos confiáveis. Esses e-mails geralmente contêm links ou anexos maliciosos que, quando clicados ou abertos, direcionam os usuários para sites falsos ou instalam malware em seus dispositivos.

Além disso, os invasores também podem realizar ataques de pharming, onde redirecionam o tráfego de um site legítimo para um site falso controlado por eles. Isso pode ser feito por meio de técnicas como envenenamento de cache DNS ou comprometimento de servidores de nomes de domínio. Outra tática comum é o *spoofing* de sites, onde os invasores criam réplicas de sites legítimos, como bancos ou redes sociais, com o objetivo de coletar informações de login e outras informações pessoais dos usuários.

Para ter sucesso, os invasores dependem fortemente de métodos de engenharia social. Eles frequentemente utilizam táticas que geram urgência ou medo nos usuários, como alegações de que suas contas serão suspensas se não tomarem medidas imediatas, ou se fazem passar por figuras de autoridade para ganhar a confiança dos usuários.

O phishing, é uma ameaça de oportunidade igual que pode atingir desktops, laptops, tablets e smartphones. Embora vários navegadores de internet possam identificar se um link é seguro, sua desconfiança é a melhor defesa contra o phishing. Ao verificar e-mail, ler postagens do Facebook ou jogar online, certifique-se de identificar sinais de phishing e tente usar computadores seguros. (MALWAREBYTES, [s/d]).

Os ataques de Negação de Serviço Distribuído (DDoS) representam uma das formas mais perigosas de ataques cibernéticos, capazes de interromper ou prejudicar significativamente a disponibilidade de serviços online. Esses ataques são projetados para sobrecarregar os recursos de um sistema alvo, como servidores web, redes ou aplicativos, tornando-os inacessíveis para usuários legítimos. (CLOUDFLARE, [s/d]).

Existem diversos tipos de ataques DDoS, cada um com suas características e métodos de execução. Entre os mais comuns estão os ataques de amplificação, os ataques de saturação de largura de banda e os ataques de exaustão de recursos. (CLOUDFLARE, [s/d]).

Os ataques de amplificação exploram vulnerabilidades em protocolos de comunicação, como o Protocolo de Controle de Transmissão (TCP) e o Protocolo de Inicialização de Sessão (SIP), para enviar pacotes de dados falsificados para servidores de terceiros.

Esses servidores, por sua vez, respondem ao alvo do ataque com uma grande quantidade de dados, amplificando o volume do tráfego direcionado ao sistema sob ataque.

Já os ataques de saturação de largura de banda envolvem o envio massivo de tráfego de rede legítimo para o sistema alvo, consumindo toda a largura de banda disponível e impedindo que usuários legítimos acessem os serviços hospedados nesse sistema. Esses ataques geralmente são conduzidos por botnets, redes de dispositivos comprometidos controladas remotamente pelos invasores.

Por fim, os ataques de exaustão de recursos visam esgotar os recursos computacionais do sistema alvo, como CPU, memória e conexões de rede. Isso pode ser feito por meio de solicitações de serviço legítimas, mas excessivas, que consomem todos os recursos disponíveis e tornam o sistema inoperável para usuários legítimos.

O impacto de um ataque DDoS pode ser devastador para organizações e serviços online. Além das perdas financeiras associadas à interrupção das operações comerciais, os ataques DDoS também podem causar danos à reputação e confiança dos clientes. Em setores críticos, como saúde, finanças e serviços de emergência, a disponibilidade ininterrupta dos serviços online é essencial para garantir o bem-estar e a segurança do público.

Para mitigar os riscos associados aos ataques DDoS, as organizações podem implementar uma variedade de medidas de segurança. Isso inclui a configuração adequada de firewalls e filtros de rede para bloquear tráfego malicioso, a implementação de Sistemas de Detecção de Intrusão (IDS) e prevenção de intrusão (IPS) para identificar e responder rapidamente a atividades suspeitas, e a utilização de serviços especializados de mitigação de DDoS, que podem absorver e filtrar o tráfego malicioso antes que ele alcance o sistema alvo.

O *ransomware* é um tipo de software mal-intencionado, ou malware, que ameaça destruir e bloquear dados ou sistemas essenciais até que um resgate seja pago. A maioria dos ransomware visava indivíduos, mas o ransomware operado por humanos, que tem como alvo de organizações, tornou-se mais recente uma ameaça maior e mais difícil de lidar com. O ransomware, que é executado por humanos, permite que um grupo de invasores obtenha acesso a uma rede comercial de uma organização. Alguns ataques desse tipo são tão sofisticados que os invasores podem estimar o custo do resgate usando os documentos financeiros internos que descobriram. (MICROSOFT [s/d]).

O ransomware dá aos criminosos a capacidade de bloquear seu computador de qualquer lugar. Depois, ele exibe uma janela pop-up informando que seu computador está bloqueado e você não poderá usá-lo. Em seguida, ele cobra um valor em dinheiro pelo resgate, normalmente usando a moeda virtual "*Bitcoin*". É quase impossível rastrear o criminoso que pode finalmente receber o valor exigido. Uma unidade monetária online chamada *BiTCoin* (BTC), criada em 2009, permite a transferência anônima de valores. A Bitcoin, que foi criada por Nakamoto, é uma moeda descentralizada, o que significa que não tem uma autoridade central. Assim, as operações de Bitcoins são criadas por uma rede de compartilhamento P2P, conhecida como Ponto a Ponto (MICROSOFT, 2016 in (CANDIDO, FLORIAN, BORGES, 2023).

O método mais simples de espalhar um *Ransomware* é por meio de um e-mail de spam, que normalmente contém anexos maliciosos ou links que levam a uma página falsa. Para induzir a sua vítima, os cibercriminosos usam a Engenharia Social para enviar spam com mensagens alarmantes que atraem o seu interesse, como avisos de entrega de correio, advertências de infrações de trânsito, declarações fiscais e promessas de prêmios milionários (AFRIKATEC, 2017; CIO 2017 in CANDIDO, FLORIAN, BORGES, 2023).

Outro método é quando há vulnerabilidade do sistema operacional, o *malware* aproveita uma vulnerabilidade do Windows que permite o protocolo de compartilhamento de arquivos SBM executar código remotamente. O *Ransomware* pode se espalhar rapidamente em qualquer máquina vulnerável da rede (TECNOBLOG, 2017 in (CANDIDO; FLORIAN; BORGES, 2023).

Um tipo de página que direciona o tráfego de um site para conteúdo malicioso é o TDS (*Traffic Distribution System).* Ao clicar em um link em um site, o usuário seja redirecionado para um fornecedor TDS. Este fornece o clique a empresas que desejam divulgar seus produtos ou serviços, bem como a cibercriminosos que desejam espalhar ameaças de *Ransomware* por sistema de distribuição de tráfego (AFRIKATEC, 2017; CIO 2017 in CANDIDO; FLORIAN; BORGES, 2023).

Para esses tipos de ataques não há uma solução em curto prazo para o fim do *Ransomware.* A melhor maneira de prevenir os ataques é evitar e bloquear os ativos da rede. Isso é um esforço importante que pode ser feito para proteger os dados, que são o que mais importa para as organizações.

3 ENGENHARIA SOCIAL: TÁTICAS DE MANIPULAÇÃO PSICOLÓGICA, PERFIL DAS VÍTIMAS E ESTRATÉGIAS DE PREVENÇÃO E CONSCIENTIZAÇÃO CONTRA OS ATAQUES MALÉFICOS EM REDES.

A engenharia social é uma abordagem mais antiga do que a informática em si. É uma maneira de controlar os sentimentos e a mente de uma pessoa para que ela agisse de acordo com seus próprios desejos (PERALLIS, [s/d]).

As organizações ao adotarem medidas preventivas e promover a conscientização sobre segurança cibernética, elas podem fortalecer sua resiliência contra-ataques de engenharia social e proteger seus ativos digitais de forma mais eficaz.

Esta seção apresenta as táticas de manipulação psicológica, o perfil das vítimas e vulnerabilidade humana e algumas estratégias de prevenção e conscientização contra os ataques maléficos em redes.

3.1 Táticas de Manipulação Psicológica

As táticas de manipulação psicológica são um aspecto fundamental da engenharia social, pois os invasores exploram as vulnerabilidades emocionais e cognitivas das pessoas para obter acesso não autorizado a sistemas e informações confidenciais.

Essas táticas são habilmente projetadas para induzir as vítimas a agirem de maneira impulsiva e desconsiderar sua vigilância usual, facilitando assim o sucesso dos ataques cibernéticos. Algumas das táticas mais comuns são: urgência e medo, autoridade falsa, reciprocidade, curiosidade e confiança (PERALLIS, [s/d]).

Com relação a urgência e medo os invasores utilizam ferramentas persuasivas para induzir as vítimas a agirem rapidamente, sem pensar criticamente sobre a autenticidade da solicitação. Por exemplo, um e-mail de *phishing* pode afirmar que a conta do usuário será suspensa se ele não clicar em um link fornecido imediatamente para "verificar" suas credenciais.

Na tática da autoridade falsa, os invasores se fazem passar por figuras de autoridade, como representantes de instituições financeiras, funcionários do governo ou administradores de sistemas. Ao atribuir falsamente autoridade, os invasores buscam ganhar a confiança das vítimas e persuadi-las a fornecer informações sensíveis ou realizar ações prejudiciais (PERALLIS, [s/d]).

A reciprocidade é uma técnica psicológica na qual as pessoas tendem a sentir-se obrigadas a retribuir um favor ou gesto positivo. Os invasores podem explorar essa tendência oferecendo algo de valor aparentemente gratuito, como um brinde ou uma oferta especial, em troca de informações pessoais.

A curiosidade é uma emoção poderosa que os invasores frequentemente exploram para induzir as vítimas a clicarem em links maliciosos ou abrir anexos suspeitos. Os e-mails de *phishing* muitas vezes incluem títulos intrigantes ou informações misteriosas para despertar a curiosidade das vítimas e incentivá-las a tomar a ação desejada.

No entanto, invasores podem tentar ganhar a confiança das vítimas ao criar um ambiente aparentemente seguro e familiar. Isso pode ser feito por meio de mensagens personalizadas que parecem vir de amigos ou colegas de trabalho, ou usando logotipos e marcas conhecidas para criar uma falsa sensação de legitimidade.

Essas táticas de manipulação psicológica são apenas alguns exemplos do vasto arsenal utilizado pelos invasores na engenharia social. Ao compreender essas técnicas e os gatilhos emocionais subjacentes, as organizações e os indivíduos podem estar melhor preparados para reconhecer e resistir aos ataques de engenharia social, fortalecendo assim sua postura de segurança cibernética.

3.2 Perfil das Vítimas e Vulnerabilidades Humanas

Compreender o perfil das vítimas de engenharia social e suas vulnerabilidades humanas é essencial para desenvolver estratégias eficazes de prevenção e proteção contra-ataques cibernéticos. Existem diversos fatores que influenciam a suscetibilidade de uma pessoa a ser alvo de manipulação por parte dos invasores.

São eles: nível de educação e experiência em tecnologia, cargo profissional e acesso a informações sensíveis, predisposição emocional e tendências comportamentais, fatores culturais e sociais, confiança no ambiente online. (COMPUGRAF, [s/d]).

O nível de educação e a experiência em tecnologia de uma pessoa podem influenciar sua capacidade de reconhecer e resistir a ataques de engenharia social. Indivíduos com maior conhecimento técnico podem estar mais conscientes das ameaças cibernéticas e ser mais cautelosos ao interagir com solicitações suspeitas.

Funcionários de cargos mais altos em uma organização, especialmente aqueles com acesso a informações sensíveis, podem ser alvos mais atrativos para os invasores. Os invasores podem visar indivíduos com poder de tomada de decisão ou acesso a dados financeiros ou de clientes, na esperança de obter informações valiosas ou realizar ações prejudiciais em nome da organização.

As vulnerabilidades humanas, como confiança excessiva, desejo de ajudar os outros, curiosidade ou medo, podem tornar as pessoas mais propensas a serem manipuladas por invasores. Por exemplo, uma pessoa pode ser mais suscetível a clicar em um link malicioso se estiver se sentindo pressionada ou preocupada com a possibilidade de perder acesso a uma conta.

Os fatores culturais e sociais também desempenham um papel na susceptibilidade de uma pessoa à engenharia social. Normas culturais que enfatizam a cortesia, o respeito pela autoridade ou a confiança interpessoal podem ser exploradas pelos invasores para manipular as vítimas.

Em um ambiente online cada vez mais interconectado, muitas pessoas tendem a confiar nas plataformas digitais e nas comunicações eletrônicas, sem questionar sua autenticidade. Essa confiança pode ser aproveitada pelos invasores, que se passam por entidades confiáveis para enganar as vítimas e obter informações sensíveis.

Compreender essas características e vulnerabilidades das vítimas de engenharia social é crucial para desenvolver estratégias de prevenção eficazes. As organizações podem implementar programas de treinamento de segurança cibernética que eduquem os funcionários sobre os riscos da engenharia social e incentivem a adoção de comportamentos seguros online. Além disso, é importante promover uma cultura organizacional que valorize a segurança da informação e encoraje a colaboração entre os membros da equipe para identificar e relatar possíveis ameaças. Ao abordar essas vulnerabilidades humanas, as organizações podem fortalecer sua resiliência contra os ataques cibernéticos e proteger seus ativos digitais de forma mais eficaz.

3.3 Prevenção e Conscientização contra os ataques maléficos em redes

A prevenção e a conscientização são componentes essenciais na defesa contra-ataques de engenharia social.

Ao educar os usuários sobre os perigos e estratégias de defesa, as organizações podem fortalecer sua postura de segurança cibernética e reduzir significativamente o risco de sucesso de ataques cibernéticos baseados em engenharia social como: programas de treinamento em segurança cibernética, simulações de *phishing, workshops* de conscientização e campanhas educacionais. (CLEARSALE, [s/d]).

As organizações podem implementar programas de treinamento em segurança cibernética para educar os funcionários sobre os diferentes tipos de ataques de engenharia social, como *phishing, pretexting e tailgating.* Esses programas devem abordar os sinais de alerta de possíveis ataques, incentivar a adoção de práticas seguras de navegação na web e fornecer orientações sobre como relatar atividades suspeitas.

As simulações de phishing são uma ferramenta eficaz para testar a conscientização e a prontidão dos funcionários em reconhecer e relatar tentativas de *phishing*. Ao enviar e-mails simulados de *phishing* para os funcionários e monitorar suas respostas, as organizações podem identificar áreas de fraqueza na conscientização e implementar medidas corretivas, como treinamento adicional ou reforço de políticas de segurança.

Workshops de conscientização podem ser realizados regularmente para fornecer informações atualizadas sobre as últimas tendências e ameaças em segurança cibernética. Esses workshops podem incluir estudos de caso de ataques de engenharia social bem-sucedidos, demonstrações de técnicas de phishing, estratégias de defesa recomendadas e criação de uma cultura de segurança.

As organizações podem lançar campanhas educacionais sobre segurança cibernética para sensibilizar os funcionários sobre os riscos e consequências de ataques de engenharia social. Isso pode incluir a distribuição de materiais educacionais, como cartazes, panfletos e vídeos, que destacam a importância da segurança cibernética e fornecem dicas práticas para proteger contra-ataques.

Promover uma cultura organizacional que valorize a segurança da informação e encoraje a colaboração entre os membros da equipe é fundamental para fortalecer a prevenção contra-ataques de engenharia social. Os funcionários devem se sentir capacitados e incentivados a relatar atividades suspeitas e buscar orientação sempre que surgirem dúvidas sobre a autenticidade de uma solicitação ou comunicação online.

Ao adotar essas medidas preventivas e promover a conscientização sobre segurança cibernética, as organizações podem fortalecer sua resiliência contra-ataques de engenharia social e proteger seus ativos digitais de forma mais eficaz. A conscientização dos funcionários e a adoção de práticas seguras de navegação na web são componentes essenciais de uma estratégia de segurança cibernética abrangente e proativa.

4 ASPECTOS LEGAIS E A ÉTICA EM SEGURANÇA CIBERNÉTICA

A legislação e a ética desempenham papéis fundamentais na proteção dos dados e na promoção de práticas responsáveis no ambiente digital. As leis de privacidade e proteção de dados, como o *General Data Protection Regulation*(GDPR) na União Europeia e a Lei de Proteção de Dados Pessoais(LGPD) no Brasil, estabelecem diretrizes claras para o tratamento de informações pessoais, exigindo consentimento transparente dos usuários e impondo penalidades por violações.

A integração eficaz de legislação e ética na segurança cibernética promove a confiança do público, protege os direitos individuais e estimula a adoção de práticas seguras por parte das organizações e profissionais do setor. Ao cumprir as leis e aderir aos mais altos padrões éticos, as empresas e os profissionais de segurança cibernética contribuem para um ambiente digital mais seguro e ético para todos os usuários.

4.1 Leis de Privacidade e Proteção de Dados

As leis de privacidade e proteção de dados desempenham um papel fundamental na regulação do uso e da proteção das informações pessoais no ambiente digital. Elas estabelecem diretrizes claras para as organizações em relação à coleta, armazenamento, processamento e compartilhamento de dados pessoais, visando garantir a privacidade e a segurança dos indivíduos. Um dos marcos mais significativos nesse campo é o Regulamento Geral de Proteção de Dados (GDPR), implementado pela União Europeia em 2018 (BRASIL, 2018).

O GDPR é uma legislação abrangente que define padrões rigorosos para a proteção de dados pessoais dentro da União Europeia e também se aplica a organizações fora da UE que processam dados de cidadãos europeus. Ele estabelece uma série de princípios fundamentais, como o princípio da transparência (que exige que as organizações forneçam informações claras e acessíveis sobre como os dados são usados), o princípio da minimização de dados (que preconiza a coleta apenas dos dados estritamente necessários para a finalidade específica) e o princípio da prestação de contas (que exige que as organizações demonstrem conformidade com o regulamento) (BRASIL, 2018).

O GDPR também confere aos titulares de dados diversos direitos, incluindo o direito de acessar, corrigir, apagar e transferir seus dados pessoais, bem como o direito de objetar ao processamento de seus dados em certas circunstâncias.

As penalidades por violações do GDPR podem ser substanciais, alcançando até 4% do faturamento global anual de uma organização ou 20 milhões de euros, o que for maior (BRASIL, 2018).

A LGPD é uma legislação brasileira criada em 14 de agosto de 2018, que segue princípios semelhantes ao GDPR, estabelecendo diretrizes para o tratamento de dados pessoais por organizações dentro do país.

Assim como o GDPR, a LGPD confere aos titulares de dados diversos direitos, como o direito de acesso, correção, exclusão e portabilidade de seus dados pessoais.

A LGPD também impõe penalidades significativas para violações, incluindo multas que podem chegar a 2% do faturamento da empresa no Brasil, limitadas a um total de 50 milhões de reais por infração (BRASIL, 2018).

4.2 Responsabilidade Legal e Ética dos Profissionais de Segurança Cibernética

Os profissionais de segurança cibernética desempenham um papel crucial na proteção dos sistemas de informação e na mitigação de ameaças cibernéticas. No entanto, essa responsabilidade vem acompanhada de obrigações legais e éticas que devem ser observadas para garantir práticas adequadas e conduta profissional. Alguns aspectos em detalhes são: proteção de sistemas e dados, resposta a incidentes de segurança, ética na condução de atividades profissionais, formação e educação contínua e colaboração e compartilhamento de informações. (NETEXPERTS, [s/d]).

Os profissionais de segurança cibernética têm a responsabilidade legal e ética de proteger os sistemas de informação e os dados confidenciais contra acessos não autorizados, modificações indevidas e destruição maliciosa. Isso inclui a implementação de medidas de segurança adequadas, como firewalls, sistemas de detecção de intrusão, criptografia e controle de acesso, bem como a realização de auditorias regulares para identificar e mitigar vulnerabilidades. (NETEXPERTS, [s/d]).

Em caso de incidentes de segurança, os profissionais de segurança cibernética têm a responsabilidade de responder de maneira rápida e eficaz para conter e remediar os danos causados.

Isso pode envolver a investigação da origem e impacto do incidente, a implementação de medidas corretivas para evitar sua recorrência e a notificação adequada das partes afetadas, conforme exigido por leis e regulamentos aplicáveis.

Os profissionais de segurança cibernética devem aderir a padrões éticos rigorosos em todas as suas atividades profissionais, incluindo a divulgação responsável de vulnerabilidades, o respeito à privacidade dos indivíduos durante investigações e a conformidade com políticas organizacionais e regulamentações aplicáveis. Isso requer uma compreensão abrangente das implicações éticas de suas ações e a capacidade de tomar decisões éticas em situações complexas e desafiadoras.

Os profissionais de segurança cibernética têm a responsabilidade de buscar continuamente o aprimoramento de suas habilidades e conhecimentos, acompanhando as últimas tendências e desenvolvimentos no campo da segurança cibernética e participando de programas de formação e educação contínua.

Isso não apenas os capacita a enfrentar as ameaças emergentes de forma eficaz, mas também reforça seu compromisso com a excelência profissional e a responsabilidade ética.

Os profissionais de segurança cibernética também têm a responsabilidade de colaborar com colegas de profissão, compartilhar informações e melhores práticas, e contribuir para o avanço da comunidade de segurança cibernética como um todo.

Isso fortalece a capacidade coletiva de responder a ameaças cibernéticas e promove uma cultura de segurança cibernética baseada na colaboração e na troca de conhecimentos.

5 SUGESTÕES DE TRABALHOS FUTUROS

À medida que a tecnologia evolui novas ameaças cibernéticas surgem, há uma necessidade crescente de pesquisas contínuas e desenvolvimento de técnicas para análise e mitigação de ataques cibernéticos. Algumas áreas promissoras para trabalhos futuros incluem: Análise de ameaças emergentes, estudos de caso e análises pós-incidente, avaliação de vulnerabilidades e testes de penetração e educação e conscientização.

A investigação aprofundada de ameaças cibernéticas emergentes, como ataques baseados em Inteligência Artificial (IA) e *machine learning*, ataques cibernéticos direcionados a dispositivos IoT (Internet das Coisas) e ameaças relacionadas a tecnologias emergentes, como computação em nuvem e *blockchain* são fundamentais. Isso envolveria a análise das características dessas ameaças, seus vetores de ataque e potenciais impactos, além do desenvolvimento de estratégias de defesa adequadas.

A implementação de ferramentas avançadas de análise e detecção de ataques cibernéticos incluem sistemas de detecção de intrusão (IDS), sistemas de análise de comportamento de usuários (UBA) e ferramentas de análise forense digital. Isso envolveria a aplicação de técnicas de *machine learning* e IA para melhorar a precisão e eficácia na identificação e resposta a ameaças cibernéticas.

A realização de estudos de caso detalhados sobre ataques cibernéticos recentes incluem análises pós-incidente para identificar falhas de segurança, erros comuns e lições aprendidas. Isso forneceria insights valiosos para aprimorar as práticas de segurança cibernética e desenvolver estratégias de defesa mais robustas.

Realização de avaliações abrangentes de vulnerabilidades em sistemas e redes, seguidas de testes de penetração para identificar e explorar possíveis brechas de segurança ajudaria as organizações a entenderem melhor suas exposições a ameaças cibernéticas e tomar medidas proativas para fortalecer suas defesas.

O desenvolvimento de programas educacionais e iniciativas de conscientização para capacitar usuários finais e profissionais de segurança cibernética a reconhecer e responder a ameaças cibernéticas incluiria a criação de materiais educacionais, workshops interativos e simulações de ataques para promover uma cultura de segurança cibernética em todas as organizações e comunidades.

O estabelecimento de plataformas e fóruns de colaboração para promover o compartilhamento de informações e melhores práticas entre profissionais de segurança cibernética, organizações e agências governamentais facilitaria a rápida disseminação de informações sobre ameaças cibernéticas e promoveria a cooperação na resposta a incidente e na proteção contra ameaças cibernéticas em escala global.

6 CONCLUSÃO

Conclui-se que a partir do objetivo proposto que foi estudar diferentes técnicas de ataques cibernéticos *(phishing, ransomware, DDoS),* examinando como são executados esses ataques, identificar os vetores de ataques e analisar os danos causados as vítimas. Verificou-se que a segurança cibernética continua sendo um desafio complexo e em constante evolução. No entanto, ao adotar uma abordagem proativa, compreendendo as ameaças emergentes e colaborando efetivamente entre as partes interessadas, pode fortalecer as defesas cibernéticas e proteger os sistemas de informação contra ameaças cada vez mais sofisticadas.

Estudos no campo da segurança cibernética é uma prioridade em um mundo cada vez mais digitalizado. O desenvolvimento de programas educacionais, iniciativas de conscientização para capacitação de profissionais e a inovação contínua são fundamentais para enfrentar os desafios emergentes e proteger infraestrutura digital de forma eficaz.

Ressalta-se que os profissionais de segurança cibernética têm a responsabilidade legal e ética de proteger os sistemas de informação e os dados confidenciais contra acessos não autorizados, modificações indevidas e destruição maliciosa. Neste sentido, a Lei Geral de Proteção de Dados tem um importante papel na garantia da proteção a todos os dados cujos titulares são pessoas naturais, estejam eles em formato físico ou digital.

Trata-se de uma temática em constante evolução importante foco de pesquisas para segurança dos dados.

REFERÊNCIAS

- ANDERSON, R. **Contramedidas em segurança da informação e vulnerabilidade cibernética:** evidência empírica de empresas brasileiras. **Revista De Administração** (São Paulo), 48(4), 757–769. (2001). Disponível em: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/#. Acesso: 10 Abr. 2024
- BRASIL. PLANALTO. **Lei Geral de Proteção de Dados (LGPD).** (2018) Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso: 17 Abr. 2024.
- CANDIDO, J. W. ., FLORIAN, F. ., & BORGES, J. H. G. Segurança Da Informação Com Foco Na Propagação Iminente De Ransomware Nas Corporações. **REVISTA FOCO, *16*(5), e1766**. (2023). Disponível em: https://doi.org/10.54751/revistafoco.v16n5-024. Acesso: 20 mai. 2024.
- CLEARSALE [s/d]. **Engenharia social**: o que é e como se proteger. Disponível em: https://blogbr.clear.sale/engenharia-social-o-que-e-e-como-se-proteger Acesso: 17 Abr. 2024.
- CLOUDFLARE [s/d]. **O que é um ataque de negação de serviço (DoS)?** Disponível em: https://www.cloudflare.com/pt-br/learning/ddos/glossary/denial-of-service/ Acesso: 16 Abr. 2024.
- COMPUGRAF [s/d]. **Engenharia social**: Quem é quem neste tipo de ataque? Disponível em: https://www.compugraf.com.br/blog/engenharia-social-quem-e-quem/ Acesso: 16 Abr. 2024.
- CORTEZ IS, KUBOTA LC (2013). Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Rev Adm** (São Paulo) [Internet]. 2013Oct;48(4):757–69. Disponível em: https://doi.org/10.5700/rausp1119. Acesso: 10 Abr. 2024.
- CREMONINI, M., & NIZOVTSEV, D. (2006). Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista De Administração** (São Paulo), 48(4), 757–769. Disponível em: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/#. Acesso: 10 Abr. 2024.
- E-SAFER [s/d]. **Ética e aspectos jurídicos em cibersegurança.** Disponível em: https://e-safer.com.br/etica-e-aspectos-juridicos-em-ciberseguranca/. Acesso: 17 Abr. 2024.
- LOPES, L. (2015). **Security Officer.** Disponível em: https://www.jusbrasil.com.br/artigos/security-officer/153252634. Acesso em: 10 Abr. 2024.
- MALWAREBYTES [s/d**]. Pishing.** Disponível em: https://br.malwarebytes.com/phishing/. Acesso: 15 Abr. 2024.
- MICROSOFT [s/d]. **O que é Ransomware?.** Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-ransomware#Ransomwaredefined. Acesso: 20 mai. 2024.

- NETEXPERTS [s/d]. **Conceitos éticos que guiam as decisões de cibersegurança**. (2023) Disponível em: https://netexperts.com.br/conceitos-eticos-que-guiam-as-decisoes-de-ciberseguranca/. Acesso: 17 Abr. 2024.
- PERALLIS [s/d]. **Engenharia social, a arte de manipular os sentimentos do ser humano**. Disponível em: https://www.perallis.com/news/tudo-o-que-voce-queria-saber-sobre-engenharia-social Acesso: 16 Abr. 2024.
- SCHNEIER, B. [s/d]. *Security Officer*. Disponível em: https://www.jusbrasil.com.br/artigos/security-officer/153252634. Acesso: 17 Abr. 2024.
- VARIAN, H. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. **Revista De Administração** (São Paulo), 48(4), 757–769. (2004). Disponível em: https://www.scielo.br/j/rausp/a/tH7hv6Jh3YcdjBNgsgzfXSM/#. Acesso: 10 Abr. 2024.