SIMULAÇÕES MULTIAGENTES E *PHISHING*: EXPLORANDO A SEGURANÇA EM AMBIENTES DE NUVEM

Leonardo Nabarro Tonezer[1]

Ana Clara Matthiesen Silva[2]

Alisson Henrique de Almeida[3]

João Emmanuel D Alkmin Neves[4]

RESUMO

Este trabalho aborda o impacto de ataques de engenharia social, em especial o *phishing*, que continua sendo uma das principais ameaças à segurança cibernética, em sistemas de computação em nuvem. Com o crescimento da adoção de serviços em nuvem por empresas e indivíduos, a vulnerabilidade a esses ataques tem aumentado, uma vez que a engenharia social explora diretamente o fator humano. O objetivo é entender como essas ameaças afetam a integridade dos sistemas na nuvem e a segurança dos dados, analisando como os atacantes acumulam informações e progridem por diferentes níveis de segurança. A metodologia adotada para tal fim foi o desenvolvimento de um modelo de simulação com sistemas multiagentes, no qual usuários, atacantes e defensores interagem em um ambiente de nuvem com diferentes camadas de segurança, levando em consideração variáveis como a suscetibilidade dos usuários e as capacidades dos atacantes. Os resultados obtidos mostram que o sucesso dos atacantes está diretamente relacionado à suscetibilidade dos usuários e com as informações acumuladas de forma gradual, reforçando a necessidade de estratégias de treinamentos mais eficazes de forma mais abrangente.

PALAVRAS-CHAVES: Ciberataques; Segurança da Informação; Sistemas Multiagentes.

ABSTRACT

This work addresses the impact of social engineering attacks, particularly phishing, which remains one of the main threats to cybersecurity in cloud computing systems. With the increasing adoption of cloud services by companies and individuals, the vulnerability to these attacks has grown, as social engineering directly exploits the human factor. The objective is to understand how these threats affect the integrity of cloud systems and data security, analyzing how attackers accumulate information and progress through different security levels. The methodology adopted for this purpose was the development of a multi-agent systems simulation model, where users, attackers, and defenders interact in a cloud environment with different security layers, considering variables such as user susceptibility and the attackers' abilities. The results obtained show that the success of attackers is directly related to user susceptibility and the gradual accumulation of information, highlighting the need for more effective and comprehensive training strategies.

KEYWORDS: *Cyberattacks; Information Security; Multi-Agent Systems.*

[1] Graduando pela Faculdade de Tecnologia de Americana.

[2] Graduanda pela Faculdade de Tecnologia de Americana.

[3] Graduando pela Faculdade de Tecnologia de Americana.

[4] Doutor pela Universidade Estadual de Campinas.

1. INTRODUÇÃO

Contemporaneamente, os ataques cibernéticos estão cada vez mais presentes no cotidiano das pessoas, destacando-se entre eles as práticas de *phishing*, uma das formas mais comuns de golpe *on-line*. O *phishing* é uma técnica de engenharia social que visa enganar indivíduos para que forneçam informações confidenciais, como senhas, números de cartões de crédito e outros dados sensíveis. Nos últimos anos, esses golpes evoluíram substancialmente, utilizando recursos tecnológicos avançados como a inteligência artificial e o aprendizado profundo, para tornar as tentativas de fraude mais convincentes e difíceis de detectar. O uso dessas tecnologias permite que cibercriminosos criem áudios e vídeos falsos que imitam com precisão a voz e a aparência de uma pessoa, facilitando a obtenção de dados valiosos de suas vítimas. Além disso, a acessibilidade crescente dessas ferramentas de falsificação digital tem permitido que os ataques de *phishing* sejam disseminados em maior escala e com maior sofisticação.

Apesar de os ataques de *phishing* atingirem qualquer pessoa, observa-se que os usuários com menor familiaridade com tecnologia são os mais vulneráveis. Esse grupo tende a enfrentar dificuldades significativas ao tentar distinguir entre mensagens fraudulentas e legítimas, o que os expõe a um maior risco de cair em golpes. Esse cenário levanta a seguinte questão: Quais são as principais dificuldades encontradas pelos usuários na identificação de mensagens fraudulentas e que medidas podem ser adotadas para reduzir a incidência de golpes e melhorar a conscientização sobre a segurança digital?

Diante desse contexto, este estudo parte da hipótese de que, apesar dos esforços contínuos de grandes empresas de tecnologia, como Google, com seu serviço de *e-mail* Gmail, e Meta, com o aplicativo de mensagens *WhatsApp,* para identificar e prevenir ataques de *phishing*, a eficácia dessas medidas tende a diminuir com o crescimento exponencial da base de usuários. Isso ocorre porque, à medida que o número de usuários aumenta, surgem novas oportunidades para que cibercriminosos desenvolvam e apliquem táticas mais sofisticadas, superando as barreiras de segurança impostas por essas plataformas.

O presente trabalho científico tem como objetivo desenvolver um modelo de simulação utilizando sistemas multiagentes para analisar os diferentes tipos de ataques de *phishing* que circulam atualmente. A partir dessa análise, pretende-se investigar as estratégias mais comuns e eficazes empregadas por cibercriminosos, bem como propor soluções práticas que possam auxiliar os usuários a identificar e evitar esses golpes. O estudo também visa contribuir para o

aprimoramento das práticas de segurança da informação, especialmente no que se refere à proteção de usuários menos experientes em tecnologia.

A justificativa para a realização deste artigo está na crescente sofisticação e disseminação dos ataques de *phishing*, que afetam milhões de usuários globalmente, resultando em perdas financeiras significativas e comprometimento da privacidade e segurança das informações. Embora as grandes empresas de tecnologia estejam implementando medidas de segurança para combater esses golpes, ainda há uma lacuna na proteção de usuários que possuem menos conhecimento sobre segurança digital. Compreender as táticas utilizadas por cibercriminosos e desenvolver soluções eficazes para melhorar a conscientização e a capacidade de resposta dos usuários são passos essenciais para a mitigação desse problema. Assim, este estudo se faz relevante para contribuir com a elaboração de estratégias mais robustas de prevenção e combate aos ataques de *phishing*, tanto no âmbito pessoal quanto no institucional, promovendo um ambiente digital mais seguro para todos.

2. REFERENCIAL TEÓRICO

Este capítulo abordará os temas de Engenharia Social, *Phishing*, Sistemas Multiagentes e Computação em Nuvem. Primeiramente em Engenharia Social, será explorado seu conceito e sua importância, bem como essa tática, quando bem executada, pode quebrar defesas do mais alto nível. Em relação ao *Phishing*, serão apresentados os diferentes tipos dessa tática e como são utilizados. A seguir, em Sistemas Multiagentes, será discutido o funcionamento desses sistemas e seus benefícios. E, por fim, na seção que trata da Computação em Nuvem, serão abordados os princípios do serviço e sua segurança.

2.1. Engenharia Social

O fator humano é o mais responsável pelas falhas e perdas de informações nas empresas, conforme mencionado por Khonji, Iraqi e Jones (2013). Pela falta de conhecimento, muitos funcionários utilizam *links* maliciosos por não saber como algumas informações devem ser tratadas, como com sigilo e proteção, por exemplo, na visão de Mitnick e Simon (2003).

Segundo Sêmola (2024), usuários são os elos mais fracos em uma organização quando não são fornecidos treinamentos, deixando assim brechas para que ataques centralizados na falha do fator humano ocorram. Este fato ressalta que os usuários devem sempre estar conscientizados sobre

o processo de proteção das informações da organização.

Engenheiros sociais geralmente possuem uma gama de ferramentas e habilidades, sendo a maior delas a arte de enganar. Através disso, buscam manipular vítimas utilizando qualidades da natureza humana, principalmente, a tendência natural de ajudar e apoiar familiares ou amigos.

Ademais, engenheiros sociais são intrinsecamente charmosos, educados e agradam facilmente seus alvos, focando em garantir o acesso a quase toda, senão, toda informação. Uma boa demonstração seria um cenário em que ele manipula e direciona seu caminho a algum local interno dentro de uma empresa para, exemplificativamente, obter acesso a um computador de algum gerente.

Na atualidade da Segurança da Informação, as organizações fornecem cada vez melhores aplicações de políticas com excelentes recursos em *software* e em *hardware* com ótimas ferramentas de proteção, e ciberataques estão cada vez mais complicados de obter sucesso direto através de redes de acesso (Moura; D'Alkmin Neves, 2021).

No entanto, boa parte dos atacantes entende que o fator humano sempre terá falhas. É praticamente impossível prevenir ou até mesmo cobrir todas as falhas que um humano possa ter, e, com isso, atacantes maliciosos utilizam dessas falhas como uma vantagem (Souza *et al.*, 2024).

Conforme Lyra (2015), a cooperação dos usuários é essencial para a eficácia da segurança, isto porque eles exercem um forte impacto sobre a confidencialidade, a integridade e a disponibilidade da informação. São os próprios usuários e seus métodos de armazenamento de senhas, proteção de dados e garantia da confidencialidade quem ditam o nível de Segurança da Informação.

2.2. Phishing

Ataques de *phishing* vêm sendo utilizados há muitos anos como uma forma de conseguir dados e informação de maneira ilegal através de golpes. O *phishing* é uma técnica de persuasão, focada em um indivíduo ou em um grupo.

Este golpe pode ser modificado conforme a vítima e o cargo que a vítima possui em uma empresa, e enganar esses indivíduos acarreta ao acesso a informações sigilosas ou até mesmo, em casos específicos, à instalação de *backdoors* em *softwares*.

Para Silva (2020), o *phishing* é a técnica mais usada nos meios cibercriminosos. Sua técnica mais simplificada consiste em *e-mails* falsos que se passam por *e-mails* reais e, por ser básica e ter a

capacidade de ser enviada para milhares de pessoas ao mesmo tempo, acaba se tornando a mais popular.

Muitos atacantes utilizam dos problemas da sociedade para fortalecer seus ataques e dar mais credibilidade a eles, como por exemplo em 2020, ano em que a pandemia de covid-19 mudou rotinas e vidas de todo o planeta. Nesse período, muitos atacantes utilizavam *links* falsos de chamadas de vídeo para infectar computadores de suas vítimas.

O crescimento de golpes de *phishing* se deve ao avanço das tecnologias digitais e à dependência de plataformas *on-line* para a vida cotidiana, o que torna o *phishing* mais complicado. Além disso, o fato de os usuários se sentirem mais à vontade e se envolverem em menos comportamentos relacionados à segurança devido à sua experiência confortável em mundos virtuais. Assim como as técnicas criminosas navegam, os mecanismos de defesa também precisam mudar e eles se alienam não apenas em soluções técnicas, mas também em programas de conscientização para os usuários.

- ***Scam Phishing***

O *scam* é o método de *phishing* clássico. Em sua tradução livre, fraude, como o nome já sugere, um atacante engana a vítima com o uso da engenharia social para ter acesso a informações pessoais e dados sensíveis das vítimas.

Neste método, atacantes utilizam como estratégia majoritária *e-mails* com *links*. Cibercriminosos se passam por grandes empresas, como bancos, solicitando senhas de contas bancárias e até mesmo informações confidenciais, como documentos pessoais. Além disso, atacantes também possuem informações prévias sobre suas vítimas.

Segundo Souza e Tanaka (2023), o método mais comum de *scams* são ofertas de serviços ou produtos falsos com um preço mais acessível em relação a seus originais com o objetivo de atrair compradores gerando uma falsa sensação de estar fazendo um ótimo negócio, quando na verdade, estão caindo em golpes que fornecerão aos atacantes tanto seu dinheiro quanto seus dados sensíveis.

- ***Blind Phishing***

O *blind phishing* consiste em uma técnica de ataque massivo de *e-mails* para o maior número de vítimas aleatórias possível. As informações não são adaptadas para cada vítima como no ataque

de *phishing* original, mas ao invés, atacantes enviam informações genéricas igualmente para todas as vítimas, com o intuito de ter a legitimidade mais próxima do real que conseguirem.

Nestes tipos de ataque, frequentemente atacantes atuam como bancos ou instituições solicitando que algumas informações do usuário sejam atualizadas, como senhas, números de telefone e até mesmo os próprios *e-mails*. Com isso, um *link* malicioso é anexado ao *e-mail* solicitando o acesso para atualização do cadastro, redirecionando o usuário a uma página falsa que poderá capturar informações enviadas ou instalar backdoors no dispositivo da vítima.

De acordo com Salviano, Santos e Silva (2021), é uma das formas de ataque mais perigosas, pois tem a capacidade de atingir uma ampla gama de pessoas.

- ***Spear Phishing***

O *spear phishing* combina várias táticas da engenharia social, tanto em alvos individuais quanto em grupos específicos, desde funcionários públicos a cargos de alto nível em organizações. Através das vítimas enganadas, informações confidenciais são facilmente recolhidas, podendo acarretar a instalação de *malwares* ou a autorização de pagamentos para contas bancárias não autorizadas de terceiros.

Para Ghazal (2015), o *spear phishing* pode ser considerado muito mais perigoso que outros tipos de *phishing*, principalmente por sua dificuldade de ser detectado. A personalização de *e-mails* meticulosamente enviados os torna menos suspeitos e mais propensos a serem abertos por seus alvos. Ademais, muitas vezes os atacantes utilizam estas técnicas para obter informações adicionais relacionadas a suas vítimas.

2.3. Sistemas Multiagentes

Os sistemas multiagentes são projetados para operar em ambientes distribuídos e dinâmicos, permitindo que agentes autônomos tomem decisões localizadas enquanto cooperam para atingir objetivos comuns (Neves, 2024).

A escolha por esses sistemas se baseia em sua capacidade de dividir o processamento entre múltiplos agentes, cada qual podendo agir de forma autônoma e organizada simultaneamente.

A eficácia dos sistemas multiagentes em cenários de ataques cibernéticos foi destacada por He *et al.* (2022). Estes sistemas utilizam estratégias de controle distribuído, o que torna a detecção

de intrusões e a recuperação mais eficientes. Quando um agente autônomo é comprometido, ele pode ser isolado sem prejudicar o funcionamento geral.

Além disso, a habilidade dos agentes autônomos de se adaptarem e aprenderem permite que respondam a mudanças no ambiente em tempo real, conferindo robustez e eficiência, mesmo em contextos hostis (Neves, 2021).

A adoção de agentes autônomos, conforme discutido por Neves *et al.* (2023) e Bordini, Vieira e Moreira (2001), possibilita a observação de cenários complexos e a obtenção de resultados claros. No entanto, diferentemente dessa característica, os sistemas multiagentes permitem a análise de comportamentos interdependentes. Embora os agentes operem de forma independente, frequentemente precisam interagir, cooperar ou competir para alcançar seus objetivos.

O uso de sistemas multiagentes para essa pesquisa traz diversas vantagens, entre elas a agilidade na resolução de problemas, visto que a modelagem de sistemas multiagentes possui uma capacidade de processamento excepcional, além de melhorar a resposta a um problema, já que estão localizados em um só ambiente.

2.4. Computação em Nuvem

Cloud computing, mais conhecido como computação em nuvem no Brasil (e em sua livre tradução), refere-se a serviços pagos em que empresas com grandes centros de processamento disponibilizam seu poder operacional para uma outra organização ou indivíduo final, podendo negociar diretamente o preço e personalizar o tipo de serviço que cada cliente deseje.

Esse tipo de serviço, comumente chamado de *self-service*, consiste em fornecer ao usuário o poder de contratar mais recursos computacionais, poder de processamento e até mesmo armazenamento, podendo modificar a qualquer momento, sem a necessidade de interação humana. Modificações ou reconfigurações de *hardware* e *software* podem ser automaticamente realizadas dentro da nuvem, sendo apresentadas de forma transparente para seus usuários.

Para que um sistema deste nível seja mantido de forma exemplar, é necessário que a Segurança da Informação seja uma preocupação essencial no meio organizacional da empresa que o fornece, para principalmente proteger um patrimônio não palpável fisicamente. O vazamento de informações e estratégias de uma organização para indivíduos não autorizados e mal-intencionados pode levar ao declínio e perdas de investimentos.

De acordo com Couto *et al.* (2022), e Camargo (2023), a Segurança da Informação é

fundamentada em três pilares principais que complementam sua plena ideia, sendo estes:

- A confidencialidade (ou exclusividade), que garante os limites de acesso da informação somente a pessoas autorizadas.
- A integralidade, que garante que a informação permaneça completa e impede qualquer modificação não permitida de dados.
- A disponibilidade, que garante que a informação esteja sempre disponível para aqueles com a devida permissão.

3. MATERIAL E MÉTODOS

A metodologia do projeto teve início com uma pesquisa bibliográfica e exploratória. O material desenvolvido baseia-se em artigos científicos relacionados ao tema: Engenharia Social, *Phishing*, Sistemas Multiagentes e Computação em Nuvem, com o objetivo de embasar o desenvolvimento do modelo proposto.

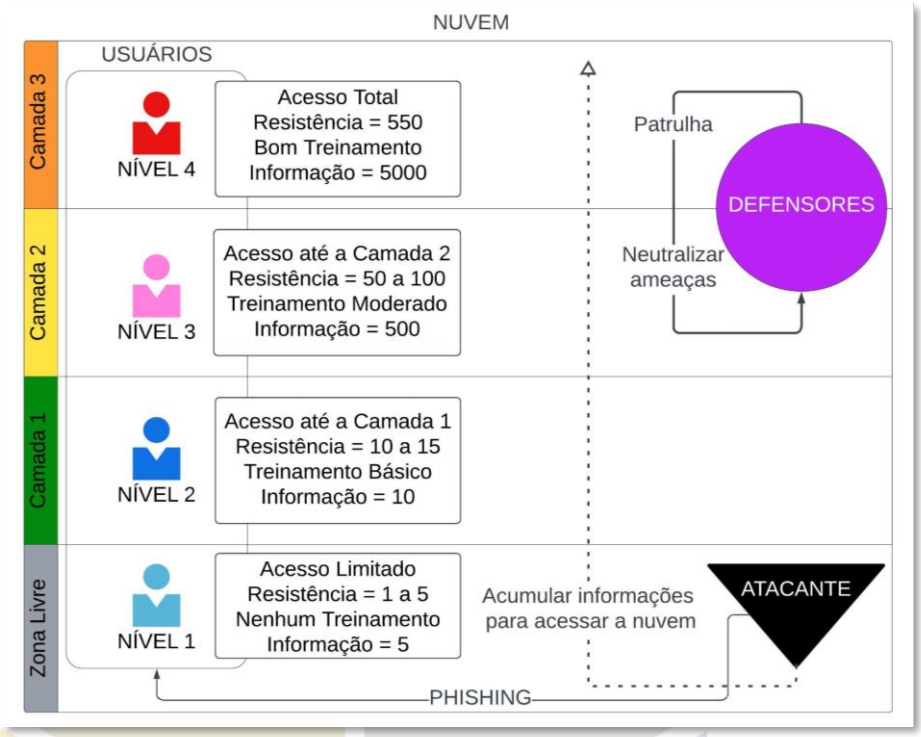
A partir destas pesquisas, realizadas por meio da leitura e análise cuidadosa dos materiais relacionados, encontrados utilizando os principais mecanismos de busca de materiais acadêmicos, como Google Acadêmico, IEEE Xplore, entre outras bases, foi possível compreender os conceitos necessários para os próximos passos do desenvolvimento deste trabalho.

Para implementar a simulação, optou-se pela utilização da ferramenta *NetLogo,* uma ferramenta amplamente utilizada para modelagem de sistemas complexos e simulação com sistemas multiagentes. A escolha do *NetLogo* se deve à sua flexibilidade e simplicidade, permitindo a criação de modelos complexos de forma intuitiva, além de sua capacidade de simular interações entre agentes e observar o comportamento emergente no sistema.

Como a pesquisa foca em interações dinâmicas entre diferentes tipos de agentes, o *NetLogo* se mostrou uma ferramenta ideal para representar essas interações em um ambiente visual e acessível, possibilitando a análise de diversos cenários de ataques de *phishing* e a evolução desses ataques ao longo do tempo.

Para iniciar a configuração do ambiente simulado, foram definidas três espécies primordiais de agentes, também conhecidos como *turtles*, na ferramenta *NetLogo.* Estes agentes, exemplificados na Figura 1, representam os três tipos principais utilizados na simulação.

Figura 1 – Esquema dos agentes.



Fonte: Autores (2024)

- Usuários: Cada usuário possui propriedades como nível hierárquico, informações e suscetibilidade a ataques.
- Atacantes: Os atacantes têm como propriedades uma lista de usuários comprometidos e informações obtidas.
- Defensores: Os defensores patrulham pelos níveis de maior segurança na nuvem.

Desta forma, seguindo a configuração dos agentes, foram atribuídas as características e dados a cada espécie. Os usuários foram organizados em quatro níveis hierárquicos, que variam de 1 (maior suscetibilidade a ataques e menor acesso à nuvem) a 4 (menor suscetibilidade e maior acesso). Essa estrutura hierárquica reflete a diversidade de papeis e privilégios dentro de uma organização, com cada nível atribuído a um número específico de usuários.

Os atacantes iniciam com o mínimo de informação possível, para ser possível a análise de como seus ataques se tornam mais convincentes à medida que acumulam informações sobre o alvo. A cada ataque realizado, o agente registra o usuário na lista.

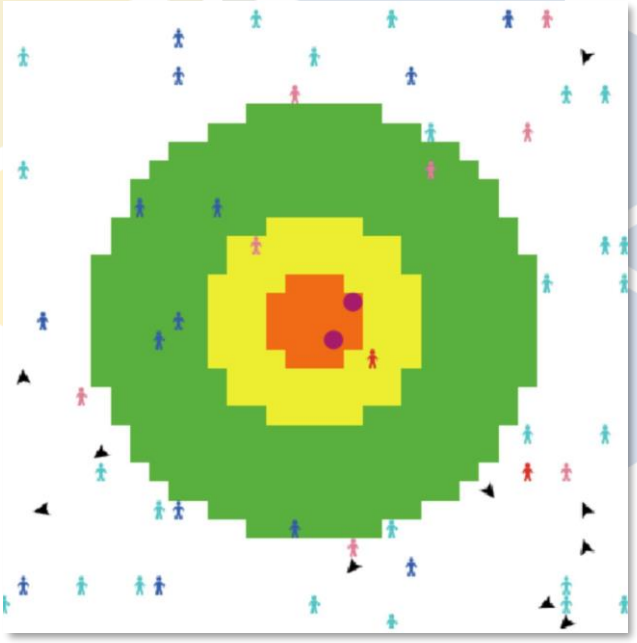
Defensores possuem o maior valor de informações, e não são suscetíveis aos ataques. Seu papel na simulação é patrulhar as áreas mais seguras e neutralizar os atacantes que encontrarem.

Em seguida, foram definidas as propriedades do ambiente em nuvem, com diferentes níveis de segurança para o acesso, simulando uma política de segurança em que os dados mais sensíveis são protegidos com mais camadas e controles de acesso mais complexos, dificultando os ataques. Na figura 1, pode-se observar o esquema do funcionamento dos agentes.

No modelo, o ambiente de nuvem é configurado com três níveis distintos de segurança, utilizando níveis de segurança para os *patches*, representados por cores (laranja, amarelo e verde). No *NetLogo, patches* são as células que compõem a grade espacial do ambiente de simulação. Cada *patch* é identificado por coordenadas e possui propriedades que podem ser modificadas ao longo do tempo, permitindo a modelagem de dinâmicas de ambiente. Além de interagirem com os agentes, os *patches* possibilitam a representação de variáveis ambientais relevantes ao contexto do estudo.

À medida que a distância do centro da nuvem aumenta, o nível de segurança diminui, simulando as diversas camadas de segurança e com cada complexidade, a região central contendo os *patches* com a maior proteção e restrição de acesso. A área mais externa, representada pela cor branca, foi atribuída como uma região de livre acesso, sendo redes abertas, locais públicos e a própria Internet. A simulação desse cenário pode ser observada na Figura 2.

Figura 2 – Captura de tela da simulação.



Fonte: Autores (2024)

Cada uma das áreas de segurança exige um valor de informações para liberar o acesso ao agente, consequentemente quanto maior o nível de segurança, mais informações necessárias para o

acesso.

Com o ambiente pronto, a simulação pode ser iniciada e os agentes irão realizar os comportamentos que lhes foram atribuídos. Os atacantes realizam o comportamento que será o elemento central dessa análise e seu objetivo principal é atacar os usuários para obter informações, para com elas aprimorar seu próximo ataque.

O sucesso de um ataque é determinado pela comparação entre o nível de informação do atacante e a suscetibilidade do alvo, replicando a forma como ataques evoluem e se tornam mais sofisticados ao longo do tempo. Essa é uma tática comumente usada em golpes de *spear phishing*, onde os criminosos têm o objetivo de obter informações de usuários específicos, geralmente com menor suscetibilidade a ataques mais simples. Ilustrado no Pseudocódigo 1, está o algoritmo utilizado na simulação.

Pseudocódigo 1 - Algoritmo de ataque utilizado nas simulações.

```
Selecionar alvo aleatório entre usuários próximos
Se alvo não estiver na lista de comprometidos então
    atacar
    Comparar informações com suscetibilidade do alvo
    Se valor das informações forem suficientes então
        Ataque bem-sucedido
        Somar informações do alvo às informações do atacante
        Adicionar alvo à lista de usuários comprometidos
    senão
        Ataque falhou
        Mudar a direção e reiniciar ataque
fim se
```

Fonte: Autores (2024)

Este comportamento simula os usuários adquirindo informações cada vez mais relevantes para incrementar seus golpes, e a aquisição de informações que possibilitam o acesso aos níveis seguros da nuvem.

Assim como os atacantes, os usuários e defensores também receberam ações que irão realizar: usuários irão se movimentar pelas áreas onde têm permissão de acesso e os defensores irão

patrulhar entre as áreas de segurança em busca de atacantes para neutralizá-los.

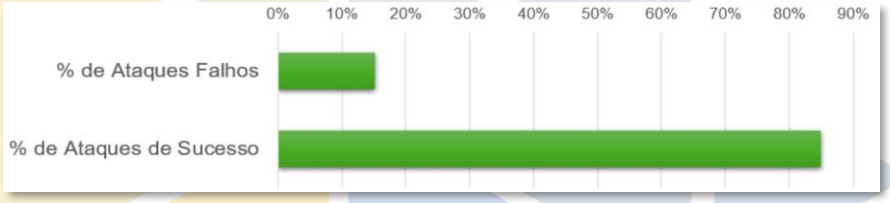
O modelo possibilita a análise e como os atacantes podem acumular informações ao longo do tempo para tornar seus golpes mais efetivos e elaborados para que sobressaiam mesmo entre as pessoas mais preparadas, pois eles aparentam transmitir mensagens autênticas.

4. RESULTADOS E DISCUSSÃO

Com o modelo desenvolvido, foi possível observar e extrair os dados da simulação em funcionamento. Com os dados adquiridos, resultados consistentes foram recolhidos, destacando-se por sua clareza e relevância para a investigação proposta, possibilitando uma análise detalhada.

Primeiramente, observou-se que o número médio de dados coletados por atacantes ao longo do tempo foi de aproximadamente 3.303. Ataques bem-sucedidos apresentaram uma taxa de cerca de 84,91%, enquanto os ataques malsucedidos registraram uma taxa de apenas 15,09%. Estes resultados podem ser visualizados em forma gráfica na Figura 3.

Figura 3 – Relação de ataques falhos e bem-sucedidos.



Fonte: Autores (2024)

Além das falhas dos próprios atacantes, durante as simulações os defensores identificaram e neutralizaram 74% dos atacantes antes de alcançarem o nível de segurança 3 da nuvem, enquanto apenas 26% dos invasores conseguiram acessar o servidor em nuvem com sucesso, como demonstrado na Figura 4.

Figura 4 – Relação de atacantes neutralizados e atacantes que não foram detectados.

Fonte: Autores (2024)

Essas condições foram mantidas constantes para garantir a comparabilidade dos dados e a robustez dos resultados, estes que uma vez obtidos, proporcionaram um discernimento mais claro sobre a dinâmica entre atacantes e defensores.

A simulação foi executada 100 vezes com as configurações explanadas na metodologia e, para os testes, a cada execução foram inicializados 10 atacantes com o valor mínimo de informações e 50 usuários de diferentes níveis e suscetibilidade variada. Destes 50 usuários, foram distribuídos 25 usuários no nível 1, 15 usuários no nível 2, 8 usuários no nível 3, e 2 usuários no nível 4, além de serem incluídos 2 defensores que patrulhavam ativamente o ambiente.

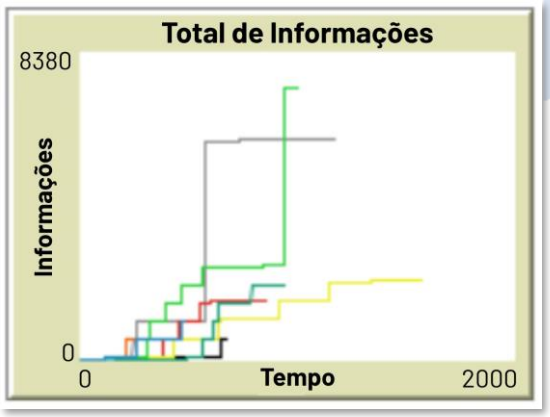
Mesmo que, durante as simulações, a maioria dos atacantes foram neutralizados antes do nível mais alto de segurança, em 97% das simulações a área mais segura da nuvem foi invadida por ao menos um atacante, evidenciando vulnerabilidades, mesmo com defesa e treinamento básicos.

Outros dados extraídos ao longo das simulações foram o acúmulo médio de informações obtidas pelos atacantes. Esses dados, extraídos como um gráfico diretamente da ferramenta NetLogo, mostram que os atacantes começaram a obter informações de forma gradual, com um crescimento acentuado nas fases intermediárias, antes da implementação das defesas mais eficazes.

O padrão observado indica que os atacantes se tornam mais eficazes à medida que acumulam informações, comprometendo os usuários, mesmo com a maior resistência.

A curva do gráfico, que pode ser observada na Figura 5, mostra um aumento lento no início, seguido por crescimento rápido e estabilização após a neutralização de parte dos invasores. Essa é uma tendência que reforça ainda mais as defesas nos estágios iniciais de um ataque, dificultando a coleta de informações até um limite crítico, reduzindo assim a eficácia do invasor bem antes que esses limites de comprometimento possam ser alcançados.

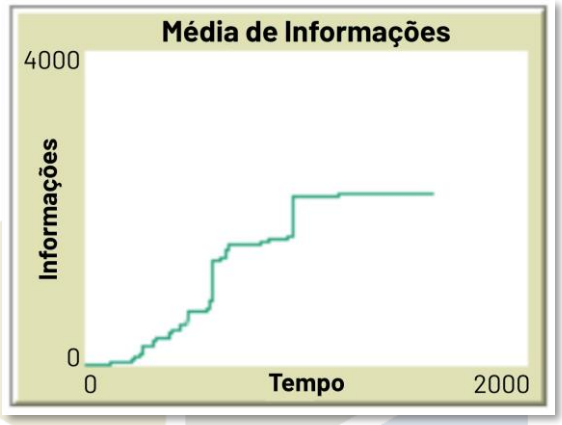
Figura 5 – Gráfico da quantidade total de informações acumuladas pelos atacantes em relação ao tempo.



Fonte: Autores (2024)

O gráfico apresentado na Figura 6 demonstra a média do acúmulo de informações obtidas pelos atacantes, demonstrando o crescimento gradual ao longo das simulações. Este gráfico reforça a hipótese de que os atacantes se tornam mais eficazes à medida que acumulam dados, até que um ponto de estabilização seja atingido, onde os ataques bem-sucedidos são neutralizados de forma mais eficiente pelos defensores. A média reflete o impacto acumulado dos ataques bem-sucedidos e o papel das defesas em mitigar o crescimento exponencial dessas ameaças.

Figura 6 – Gráfico da quantidade média de informações acumuladas pelos atacantes em relação ao tempo.



Fonte: Autores (2024)

Esses resultados fornecem uma base sólida para compreender o comportamento dos atacantes e a evolução da eficácia das defesas, destacando a importância de um monitoramento contínuo e melhorias nas estratégias de prevenção contra-ataques de *phishing* em ambientes de nuvem.

5. CONCLUSÃO

Em síntese, a proteção de dados confidenciais é essencial, com um valor que excede qualquer custo de recuperação. Os resultados deste estudo reforçam a importância de investir em treinamentos e capacitação de usuários para reduzir a vulnerabilidade a ataques de *phishing*, especialmente em sistemas de nuvem.

Os achados indicam que a conscientização e o preparo contínuo dos usuários são fundamentais para mitigar os riscos representados por cibercriminosos. Assim, recomenda-se que organizações adotem não apenas políticas de segurança robustas, mas também programas

contínuos de treinamento em segurança e tecnologias avançadas de detecção para maximizar a eficácia da proteção de seus ativos.

O modelo desenvolvido, enquanto já fornece uma base sólida para a análise do comportamento dos atacantes e dos usuários, deve ser aprimorado e expandido em futuros trabalhos. Com algumas modificações e adições, como a introdução de novos tipos de ataques e variáveis comportamentais, o modelo pode ser expandido para avaliar diferentes táticas de ataque e defesa em variados contextos de segurança. Esse aprimoramento permitirá uma análise mais abrangente e detalhada, contribuindo ainda mais para a compreensão das ameaças cibernéticas e o desenvolvimento de estratégias eficazes de proteção.

Futuras pesquisas devem, portanto, explorar a eficácia de diferentes métodos de treinamento e ferramentas de segurança em uma variedade de cenários organizacionais e contextos de nuvem. Fortalecer a resiliência contra ameaças cibernéticas passa a ser não apenas uma iniciativa desejável, mas uma necessidade essencial para assegurar ambientes digitais mais seguros e protegidos. Ao aprimorar tanto o treinamento quanto as ferramentas tecnológicas, espera-se que as organizações possam lidar de maneira mais eficiente com os desafios dinâmicos do cenário de segurança atual.

REFERÊNCIAS BIBLIOGRÁFICAS

BORDINI, R. H.; VIEIRA, R.; MOREIRA, A. F. Fundamentos de sistemas multiagentes. **Anais do XXI Congresso da Sociedade Brasileira de Computação (SBC)**, [S. l.], v. 2, p. 3–41, 2001.

CAMARGO, S. M. M. **Análise técnica de um phishing de e-mail sob a luz da ferramenta phishtool**. Orientador: José Luís Zem. 2023. 33 p. Trabalho de conclusão de curso (Curso Superior de Tecnologia em Segurança da Informação) - Faculdade de Tecnologia de Americana "Ministro Ralph Biasi", Americana, 2023. Disponível em: https://ric.cps.sp.gov.br/handle/123456789/14812. Acesso em: 17 set. 2024.

COUTO, K. S.; AMORIM, Y. R.; LIMA, K. M. D.; JÚNIOR, I. G. Os Três Pilares da Segurança da Informação na Internet Chinesa. ***Journal of Technology & Information***, [S. l.], v. 2, n. 2, 2022. Disponível em: http://jtni.com.br/index.php/JTnI/article/view/41. Acesso em: 18 set. 2024.

GHAZAL, F. **Vulnerabilidade das informações empresariais através do uso de dispositivos móveis**. Orientador: Francis Kanashiro Meneghetti. 2015. 18 p. Trabalho de conclusão de curso (Especialização em Gestão Empresarial) - Programa de Pós-Graduação em Administração, Universidade Tecnológica Federal do Paraná, Curitiba, 2015. Disponível em: https://repositorio.utfpr.edu.br/jspui/handle/1/19544. Acesso em: 17 set. 2024.

HE, W.; XU, W.; GE, X.; HAN, Q.; DU, W.; QIAN, F. *Secure control of multiagent systems against malicious attacks: a brief survey.* ***IEEE Transactions on Industrial Informatics***, [S. l.], v. 18, n. 6,

p. 3595-3608, 2022. DOI: 10.1109/TII.2021.3126644.

KHONJI, M.; IRAQI, Y.; JONES, A. *Phishing Detection: A Literature Survey.* ***IEEE Communications Surveys & Tutorials****, [*S. l.], v. 15, n. 4, p. 2091-2121, 2013. DOI 10.1109/SURV.2013.032213.00009. Disponível em: https://ieeexplore.ieee.org/abstract/document/6497928. Acesso em: 1 out. 2024.

LYRA, M. R. **Governança da Segurança da Informação**. [S. l.: S. n.], 2015. *E-book* (208 p.).

MITNICK, K. D.; SIMON, W. L. **A Arte de Enganar**. [S. l.]: Pearson Education, 2003. ISBN 978-8534615167.

MOURA, T. M.; D'ALKMIN NEVES, J. E. **Análise de Segurança em Dispositivos Internet das Coisas**. Revista Interface Tecnológica, [S. l.], v. 18, n. 2, p. 15-27, 2021. Disponível em: https://doi.org/10.31510/infa.v18i2.1174. Acesso em: 8 set. 2024.

NEVES, J. E. D. A. **Modelo Baseado em Agentes para Simulação de Consumo de Energia Elétrica em Função do Comportamento Humano**. Revista Eletrônica Anima Terra, v. 12, p. 89-103, 2021. Disponível em: https://fatecmogidascruzes.com.br/pdf/animaTerra/edicao12/artigo7.pdf. Acesso em: 8 set. 2024.

NEVES, J. E. D. A. **Mineração de dados aplicada a simulação de cenários complexos em sistemas multiagentes**. Orientadores: Paulo Sérgio Martins Pedro (*in memoriam*), Marli de Freitas Gomes Hernandez. 2024. 237 p. Tese (Doutorado em Tecnologia) - Faculdade de Tecnologia, Universidade Estadual de Campinas (UNICAMP), Limeira, 2024. Disponível em: https://www.repositorio.unicamp.br/acervo/detalhe/1395946. Acesso em: 8 set. 2024.

NEVES, J. E. D. A.; PEDRO, P. S. M.; HERNANDEZ, M. F. G.; FABRI JUNIOR, L. A. ***Simulation of the Implementation of Domestic Solar Systems Using Multi-agent Systems from Web Scraping****. Smart Innovation, Systems and Technologies. 1ed.: Springer International Publishing,* 2023, v. 1, p. 88-96. Disponível em: https://doi.org/10.1007/978-3-031-04435-9_8. Acesso em: 16 set. 2024.

SALVIANO, E. M.; SANTOS, J. P. R.; SILVA, M. A. E. **Principais tipos de ataques *Phishing* e mecanismos de segurança**. Orientador: Helder Line Oliveira. 2021. 24 p. Trabalho de conclusão de curso (Curso Superior de Bacharel em Sistemas da Informação) - Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC, Brasília, 2021. Disponível em: https://dspace.uniceplac.edu.br/handle/123456789/1611?locale=pt_BR. Acesso em: 17 set. 2024.

SÊMOLA, M. **Gestão da Segurança da Informação**: Uma Visão Executiva. 2. ed. [S. l.]: GEN LTC, 2013. ISBN 978-8535271782.

SILVA, C. Golpe de Dia dos Namorados promete perfume da marca O Boticário. **TecMundo**. [S. l.],11 jun. 2020. Disponível em: https://www.tecmundo.com.br/seguranca/154072-golpe-dia-namorados-promete-perfume-marca-boticario.htm. Acesso em: 17 set. 2024.

SOUZA, A. L. O.; BASTOS, C. V.; SANTOS, P. M. S.; SOARES, N. M.; NEVES, J. E. D. **Cibersegurança na Agricultura de Precisão: Exploração à Aplicação de Medidas Preventivas**. Advances in Global Innovation & Technology, [S. l.], v. 2, p. 61-73, 2024. Disponível em:

https://doi.org/10.29327/2384439.2.2-5. Acesso em: 17 set. 2024.

SOUZA, L. C. D.; TANAKA, S. S. Estudo sobre ataques de *phishing* e suas técnicas de defesa. **Revista Terra & Cultura**: Cadernos De Ensino E Pesquisa, [S. l.], v. 39, n. especial, p. 90-95, 16 fev. 2023. Disponível em: http://periodicos.unifil.br/index.php/Revistateste/article/view/2804/2567. Acesso em: 17 set. 2024.