UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

Automatização da Consciencialização em Cibersegurança

João Pedro Francela Lopes

Mestrado em Engenharia Informática

Versão Pública

Trabalho de Projeto orientado por:
Prof. Doutor Luís Antunes

2024

Agradecimentos

Gostaria de agradecer ao meu orientador Prof. Dr. Luís Antunes, pois não teria sido possível terminar a tese sem a sua orientação, ajuda e conselhos. Agradeço também à EMVENCI e ao Alexandre Aniceto pela oportunidade de ser integrado na equipa da EMVENCI e poder trabalhar neste projeto.

Ainda no contexto da empresa, gostaria de agradecer diretamente a Vasco Lopes, Diogo Maia, Daniel Fino, Núria Santos, Bruno Aleixo e ao Oscar. Muito obrigado por estarem ao meu lado desde o primeiro dia deste estágio, tornando esta longa e difícil jornada mais fácil.

Gostava de também agradecer aos meus pais, José Andrade Lopes e Susana Maria Geraldes Francela Lopes, por todos os sacrifícios que fizeram por mim para que nunca me faltasse nada. Aos meus pais quero agradecer pelo incentivo e apoio emocional durante todos estes anos académicos, estando sempre lá tanto para os bons, como os maus momentos. Agradeço também à minha irmã Ana Daniela Francela Lopes que, mesmo quando discordávamos, sempre quis o melhor para mim, dando os melhores conselhos e sendo um exemplo a seguir.

Um grande obrigado também a todos os meus amigos e colegas que ganhei durante estes cinco anos de vida académica, como também antes dela, sou um sortudo por poder considerar-me amigo destas pessoas. Obrigado por sempre me apoiarem, fazerem-me rir e acima de tudo serem capazes de me chamar à razão quando preciso.

Por fim, gostava de agradecer à minha melhor amiga e namorada, Margarida Rodrigues Gaspar, por ser a pessoa incrível que é e por ter-me acompanhado durante todos estes anos. Estou grato por ela ser a pessoa que melhor me conhece, por ela querer sempre o meu bem e por estar sempre lá para mim, seja para rir nos melhores momentos, ou para aguentar o forte nos piores. Obrigado por todos estes anos e por todo o apoio necessário nesta jornada.

Para a minha família e amigos.

Resumo

Esta dissertação em Engenharia Informática, orientada pelo Professor Dr. Luís Antunes, e supervisionada pelo CEO da empresa EMVENCI, Alexandre Aniceto, tem como objetivo analisar e melhorar o atual simulador de *Phishing* da EMVENCI. Esta empresa, que atua na área da cibersegurança é responsável por desenvolver a *Cybersecurity Cloud*, uma plataforma *Software as a Service* (SaaS) que tem como propósito ajudar as empresas na formação dos trabalhadores quanto à sua cibersegurança.

A plataforma é constituída por diversos módulos, sendo alguns deles registo dos requisitos Regulamento Geral de Proteção de Dados (RGPD); gestor de vulnerabilidades; formação em cibersegurança (*eLearning*) e também um simulador de ataques de *Phishing*. Este último módulo será então o foco da presente dissertação, tendo como objetivo melhorá-lo. Dentro destas melhorias, inclui-se a sua automatização, tornando-o mais prático e fácil de utilizar, esperando também que estas alterações se traduzam numa maior eficiência e adaptabilidade quanto ao treino dos colaboradores.

Palavras-chave: Phishing, Educação, Simuladores, Cibersegurança, Automação

Abstract

This dissertation in Computer Engineering, supervised by Professor Dr. Luís Antunes and the CEO of EMVENCI, Alexandre Aniceto, aims to analyze and improve EMVENCI's current Phishing simulator. EMVENCI, which operates in the cybersecurity area, is responsible for developing the platform Cybersecurity Cloud, a Software as a Service (SaaS) designed to help companies train their employees about the topic of cybersecurity.

The platform consists of several modules, including handling the requirements of the General Data Protection Regulation (GDPR); vulnerability manager; cybersecurity training, also known as eLearning; and a phishing attack simulator. The focus of this dissertation will be this last module, being the main goal to improve it. This improvements will include its automation, making it more practical and easier to use. Its expected that these changes will result in a greater efficiency and adaptability in the employee training provided by the simulated attacks.

Keywords: Phishing, Awareness, Training, Cybersecurity, Automation

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

A presente dissertação em Engenharia Informática, orientada pelo Professor Doutor Luís Antunes, e supervisionada pelo CEO da empresa EMVENCI, Alexandre Aniceto, tem como objetivo melhorar o atual simulador de *Phishing* da EMVENCI através da sua automação. Esta empresa, que atua na área da cibersegurança, é responsável por desenvolver a *Cybersecurity Cloud*, uma plataforma *Software as a Service* (SaaS) que tem como propósito ajudar as empresas na formação dos trabalhadores quanto à sua cibersegurança.

A plataforma é constituída por diversos módulos, entre os quais se incluem, registo dos requisitos Regulamento Geral de Proteção de Dados (RGPD); gestor de vulnerabilidades; formação em cibersegurança (*eLearning*) e também um simulador de ataques de *Phishing*. O último módulo mencionado será o foco da presente dissertação, tendo como objetivo melhorá-lo através da sua automatização, tornando-o assim, mais prático e fácil de utilizar. Estas alterações também irão contribuir para a adaptibilidade dos simulacros, aumentando a sua eficácia e tornando-os ainda mais realistas, esperando assim que resulte numa maior eficiência no treino dos colaboradores.

1.1 Contexto

Dada a constante evolução tecnológica, existe uma maior facilidade em obter as ferramentas necessárias para a realização de ataques *online*, traduzindo-se num aumento significativo da ocorrência de ataques na área da cibersegurança.

Estima-se que os ataques realizados nesta área atinjam um custo de quase 10 triliões de euros anualmente até 2025. Uma evidência deste aumento na quantidade da ocorrência dos ataques, é o facto de em 2023, ter havido um grande aumento de ataques que tirassem proveito da inteligência artificial. Mesmo assim, houve uma forma de ataque que se destacou entre as outras, o *Phishing*, que continuou como o principal vetor de ataque [14], tornando-se ainda mais perigoso ao também tirar proveito desta tecnologia, tendo a ocorrência dos ataques de *Phishing* com o recurso a inteligência artificial aumentado cerca de 1265% em 2023 [19].

O *Phishing* tem como objetivo roubar informações sensíveis do utilizador, sendo também particularmente difícil de reconhecer devido às suas múltiplas variantes, como *Vishing*, *Whaling*, *Smishing*, entre outros [26]. Dado então à sua constante evolução, é crucial fornecer uma formação

adequada dos colaboradores para que possam identificar e lidar com as nuances deste problema, garantindo assim a sua segurança *online* e a segurança das empresas onde trabalham.

1.2 Problema

As vítimas dos ataques de *Phishing* são maioritariamente colaboradores, sendo que o atacante não tenciona obter informações sobre a vítima, mas sim sobre a empresa a que ela pertence. De forma a mitigar esse problema, as empresas investem em formações, para os trabalhadores saberem identificar este tipo de ataque, muitas vezes através de simulações de ataques, com o intuito de sinalizar os colaboradores mais propícios a serem vítimas de *Phishing*.

Ainda assim, estes simulacros apresentam algumas oportunidades de melhoria.

A primeira está relacionada com o facto de todos os colaboradores, ao serem alvos do mesmo simulacro, acabam por receber em simultâneo, exatamente o mesmo ataque em termos visuais. Isto poderá acabar por comprometer os resultados do simulacro porque caso dois colaboradores encontrem-se nesta situação, ao receber o ataque ao mesmo tempo, poderão estranhar e conversar um com o outro, percebendo de que se trata de uma tentativa de ataque. Este cenário acaba por não ser ideal pois não garante que os colaboradores são capazes de reconhecer ataques de *Phishing* de forma independente, visto que podem ter apenas detetado este ataque porque estavam juntos, ou seja, se o mesmo voltasse a acontecer e ambos estivessem isolados, podiam continuar a ser facilmente comprometidos por um atacante experiente.

Para além disso, todo o processo de gerir corretamente os colaboradores que precisam ou não de melhorar os seus conhecimentos na área da cibersegurança acaba por ser bastante demorado, sendo necessário executar múltiplos simulacros. Não só, como também é necessário haver uma extensa análise dos resultados obtidos, o que leva à necessidade de ser feita uma constante manutenção dos colaboradores e simulacros para garantir a sua eficácia.

Em consequência destas limitações, as empresas acabam por não investir no uso deste tipo de ferramentas, surgindo assim a necessidade de aprimorar a solução existente.

1.3 Objetivos

O propósito desta dissertação é capacitar uma das soluções atuais presentes na plaforma *Cybersecurity Cloud*, através da melhoria do seu módulo de simulacros de *Phishing*, permitindo a realização de simulações de ataques mais eficazes e dinâmicos.

Para isso, pretende-se capacitar o atual simulador para que possa ter a opção de escolher múltiplos conteúdos para um único simulacro, sendo estes depois enviados aleatoriamente para cada colaborador, colmatando assim um dos problemas elaborados anteriormente.

Tem-se também como objetivo a automatação deste módulo, para que o mesmo seja capaz não só de propor como também de realizar múltiplos simulacros de forma autónoma, ajustando o nível de dificuldade dos conteúdos apresentados em função dos resultados obtidos para cada colaborador.

Espera-se que a automação deste módulo reduza o tempo dedicado à análise e preparação de simulacros, proporcionando assim uma experiência mais prática para os administradores da plataforma e mais enriquecedora para cada colaborador.

As alterações propostas por este projeto serão realizadas com base num módulo já existente, capaz de realizar simulações de ataques de *Phishing* através da plataforma *Cybersecurity Cloud*.

Em suma, pretende-se realizar a análise, aprimoramento e automatização do simulador de ataques de *Phishing* da empresa EMVENCI.

1.4 Contribuições

O projeto tem como objetivo explorar os requisitos funcionais existentes e capacitar o atual simulador de *Phishing* para que este seja capaz de suportar mais do que um formato de ataque por simulacro e também, adicionar automatação ao próprio módulo, ao propor não só uma arquitetura como também os passos que devem ser tomados para a sua implementação.

1.5 Estrutura do Documento

Esta dissertação está organizada em 7 capítulos. O primeiro capítulo visa evidenciar os desafios ligados à constante evolução dos ataques de *Phishing*. Introduz também a empresa EMVENCI, responsável por uma das soluções atuais para este problema. No segundo capítulo, explora-se em maior detalhe sobre este tópico, bem como as soluções encontradas e a eficácia das mesmas. O terceiro capítulo aborda as tecnologias já existentes utilizadas para o desenvolvimento deste projeto. Em seguida, o quarto capítulo expõe o âmbito deste projeto, incluindo uma análise de todos os objetivos pretendidos para o mesmo. Já no quinto capítulo elabora-se sobre todo o delinear da solução criada, sendo a implementação da mesma abordada no sexto capítulo, onde também é incluída como foi feita toda a testagem. Finalmente no sétimo e último capítulo é exposta a conclusão sobre todo o trabalho realizado, incluindo também uma reflexão sobre possíveis melhorias que possam vir a ser implementadas.

Capítulo 2

Conceitos e Definições

Este capítulo aborda em maior detalhe o conceito de *Phishing*, incluindo uma análise de casos de estudo relacionados às medidas de combate existentes aos atques de *Phishing*.

2.1 Engenharia Social

A engenharia social é considerada como uma técnica utilizada para manipular pessoas, com o intuito de obter informações confidenciais, acesso a sistemas ou até mesmo realizar determinadas ações [5]. Esta pode ser aplicada em diversos setores da segurança da informação, e tem como objetivo explorar o elemento mais vulnerável dentro de um sistema, o ser humano. Isto acontece pois, neste contexto, apenas o ser humano possui traços comportamentais e psicológicos, o que o torna suscetível a ser manipulado por ataques de engenharia social [28]. Com isso, é possível perceber que a engenharia social é uma técnica bastante eficaz, chegando até a ser considerada pelo Centro Nacional de Cibersegurança de Portugal, como um dos maiores riscos de segurança para as pessoas [6], estando esta relacionada muitas das vezes com a forma de como os ataques de *Phishing* são realizados.

2.2 Ataques de *Phishing*

Phishing é um dos tipos de ataque mais comuns no mundo da cibersegurança. Baseia-se no envio de comunicações fraudulentas mascaradas intencionalmente pelo atacante para parecer que foram originadas por uma fonte segura. Para estes ataques, os atacantes tiram proveito da engenharia social, explorando a falsa sensação de segurança das suas vítimas, convencendo-as a submeterem as suas informações sensíveis numa plataforma controlada pelo atacante. Muitas vezes, os atacantes iniciam estes ataques através do envio de *emails* para as suas vítimas. No entanto, é importante salientar que com o avanço das novas tecnologias, cada vez mais existem novas formas de realizar estes ataques, explorando novos meios de comunicação como o *SMS*, *USB* e muitos outros. Um exemplo que suporta esta afirmação é que recentemente foi detetada a utilização de *QRCodes* como um meio de comunicação para efetuar este tipo de ataques, sendo esta variante apelidada de *Quishing* [15].

É importante mencionar que, devido à flexibilidade das novas formas dos ataques de *Phishing*, o âmbito do mesmo também tem evoluído, sendo que o objetivo já não é apenas a roubar os dados do utilizador. Ao ser adaptado ao perfil da vítima e a um contexto específico, é possível que um ataque de *Phishing* bem-sucedido seja capaz de instalar *software* malicioso no dispositivo da vítima, ou até, de extorquir dinheiro da vítima ao forjar despesas falsas.

Um exemplo comum de *Phishing* é através de um *email* malicioso. Neste a vítima é solicitada que consulte imediatamente um *website* que lhe é familiar, sendo que, ao carregar no *link* fornecido, é redirecionada para uma imitação da plataforma mencionada no *email*. Caso a vítima não repare neste detalhe, continuará com as suas ações normalmente, acreditando que está a interagir com uma entidade confiável. Daí em diante, como a plataforma utilizada é uma versão forjada pelo atacante, todas as ações feitas pela vítima estarão comprometidas, possibilitando assim a captura de dados sensíveis sem que ela se aperceba, permitindo depois escalar o ataque e tornando-o ainda mais perigoso.

2.2.1 Impacto no Mundo Empresarial

Embora os ataques de *Phishing* sejam bastante eficazes em vítimas isoladas, eles acabam por ser mais prejudiciais quando a vítima faz parte de uma empresa. Através destes, é possível extrair informações sensíveis sobre potenciais colaboradores, o que pode comprometer toda a segurança da empresa.

Consideremos o exemplo descrito anteriormente, em que agora a vítima é um funcionário de uma grande empresa que acabou de ter as suas credenciais roubadas. O atacante até pode ter pouco ou nenhum interesse sobre o trabalhador, mas através das credenciais obtidas, pode agora escalar o ataque tornando toda a empresa vulnerável.

Segundo os dados relativos a 2021, estima-se que cerca de 22% de todas as ocorrências de *data breaches* tenham sido causadas devido a ataques de *Phishing* [20]. Para além disso, cerca de 88% de todas as empresas já reportaram a ocorrência deste tipo de ataques [20], salientando assim o quão recorrentes e perigosos estes ataques são no mundo empresarial.

2.2.2 Problemas na Área da Cibersegurança

Existem inúmeras ferramentas e técnicas úteis para prevenir ataques de *Phishing*, no entanto acabam por cair no desuso. Tal acontece devido à constante falta de trabalhadores especializados na área. Estima-se que atualmente, cerca de dois terços das empresas não têm os colaboradores necessários para prevenir e resolver problemas relacionados com a cibersegurança dentro das empresas [10], e que até 2025, existam cerca de 3,5 milhões de vagas por preencher na área da cibersegurança [22].

Muitas vezes, o motivo por trás deste problema está relacionado com o facto das empresas acharem desnecessário e dispendioso investir nesta área. Acabam por não adquirir as ferramentas adequadas, nem contratar especialistas em cibersegurança, deixando assim este tipo de cargo atribuído a pessoas não qualificadas, ou até mesmo por preencher. Ainda assim, seria mais

benéfico para as empresas investirem corretamente em boas práticas de cibersegurança, visto que acabam por ter um maior prejuízo após um ataque de *Phishing* bem-sucedido.

Outro motivo para a pouca contratação de especialistas deve-se à própria falta de pessoas formadas na área. Uma das razões para isso foi o rápido avanço tecnológico que acabou por tornar a formação sobre este tópico rapidamente desatualizada. Para além disso, dada a grande variedade de tópicos em cibersegurança, é crucial ter conhecimentos sobre as múltiplas subáreas que a constituem, tais como a análise de rede, testes de penetração, gestão regular de segurança empresarial, entre muitos outros, exigindo assim um vasto conjunto de habilidades que precisam de ser dominadas. [7]

Por fim, é importante salientar que a própria área está em constante evolução, tornando-se dificil acompanhar a sofisticação e evolução de novos ataques, sendo necessário o desenvolvimento de ferramentas e soluções capazes de combater estes avanços.

2.2.3 Formas de Prevenção

Devido ao elevado número de ataques de *Phishing* e também pelos grandes danos que estes causam, algumas empresas sentem mesmo assim, a necessidade de arranjar formas de combater estes ataques. Frequentemente recorrem a três técnicas [11], sendo estas: a remoção automática de mensagens suspeitas e dos seus *websites* correspondentes; mecanismos de aviso autónomos que notificam os colaboradores quando detetam uma mensagem suspeita; e o treino comportamental durante o qual os colaboradores são ensinados a identificar e reportar este tipo de ataques.

Embora à primeira vista as opções baseadas em *softwares* de deteção automática possam parecer suficientes, é crucial lembrar que os ataques de *Phishing* são altamente dinâmicos. Devido a isto, muitas vezes estas ferramentas mostram-se bastante eficazes a identificar ataques de pequena escala ou menos sofisticados, mas acabam por não detetar ataques mais cuidadosamente planeados e direcionados a um colaborador específico. [9]

Apesar dos modelos utilizados por estes *softwares* poderem ser sempre treinados com diversos *datasets*, é importante salientar que devido à grande diversidade e constante evolução dos ataques de *Phishing*, a definição da sensibilidade destas ferramentas, como por exemplo o número de falsos-positivos identificados, ainda é um grande desafio na área da cibersegurança [3].

Aqui entra a terceira técnica, o treino comportamental de colaboradores. Este visa educar os trabalhadores para que tenham uma melhor compreensão sobre este tipo de ataques e todas as suas nuances, aprendendo também a protegerem-se contra eles. [21] Frequentemente, recorre-se a recursos educativos como vídeos ou documentos de forma a melhorar os conhecimentos dos colaboradores. Para além disso, mais recentemente são também realizados ataques simulados, nos quais se tenta recriar ao máximo o que seria um ataque real.

2.2.4 Treino Comportamental

Embora com o aumento de incidências dos ataques de *Phishing* tenha também aumentado o número de empresas que apostam no treino comportamental, esta técnica acaba por ter os seus

próprios desafios. Um deles é a falta de interesse por parte dos colaboradores envolvidos. Este desinteresse deve-se ao facto de que na maioria das vezes, o público-alvo considera todo o processo como uma tarefa secundária [27]. Para além disso, identificou-se também uma falta de motivação por parte dos colaboradores, em relação a todo o processo de aprendizagem.

Vários investigadores tentaram resolver os desafios presentes no treino comportamental. Destes destacam-se Kumaraguru e Sheng, que através de múltiplos estudos [23, 13, 12] abordaram o tópico sobre como a forma tradicional desta técnica funcionava, tentando perceber os seus problemas e como poderiam vir a ser resolvidos.

Primeiramente, analisou-se a raíz deste problema, Kumaraguru et al. (2007) concluiram que simplesmente enviar material sobre a prevenção do *Phishing* não era suficientemente eficaz [13]. Como suspeitado, o mesmo acontecia pois a maioria das pessoas já estavam acostumadas a receber esse tipo de material educativo, e como tal negligenciavam-no.

Foram então desenvolvidas duas metodologias com o objetivo de contornar o desinteresse dos utilizadores. Ambas, consideradas como tipos de aprendizagem integrada, baseiam-se em ensinar as pessoas num contexto mais prático, contrastando assim diretamente com outras formas mais tradicionais até agora praticadas [23, 12]. Até à altura, era bastante comum ser apenas apresentado um conteúdo teórico e genérico, sem contribuir de qualquer forma para um cenário mais prático.

A primeira metodologia, desenvolvida por Sheng et al. (2007), consiste num jogo no contexto da cibersegurança [23]. Este jogo tinha como objetivo permitir aos participantes aprenderem sobre conceitos úteis relacionados à prevenção de ataques de *Phishing*.

Apelidado de *Anti-Phishing Phil*, este jogo baseava-se em ensinar aos participantes boas práticas a ter ao analisar *links* de *websites*. Para além disso, tinha também a função de avaliar se os conceitos foram bem compreendidos ou não, através de uma pontuação atribuída ao colaborador. Durante este estudo, foi possível realizar uma avaliação com quase cinco mil participantes, onde se observou que cerca de 61% sentiram melhorias em identificar ataques de *Phishing*, reduzindo também drasticamente os falsos positivos.

Na segunda metodologia, Kumaraguru et al. (2009) [12] desenvolveram um sistema de aprendizagem integrada chamado *PhishGuru*. Neste sistema, é simulado um cenário em que normalmente as pessoas seriam atacadas, com o objetivo de conseguirem aprender a reconhecer possíveis tentativas de ataque.

Para isso, eram enviados aleatoriamente *emails* de *Phishing* aos participantes, os quais continham um *link* que direcionava para uma plataforma forjada e controlada por um atacante. Caso os participantes não se apercebessem e acessassem ao *link* presente no *email*, eram imediatamente avisados que falharam no simulacro. Em seguida, eram apresentados conteúdos educativos aos participantes, explicando como este tipo de ataques funciona, onde falharam, e como devem proceder para evitar cometer novamente o mesmo erro.

Neste estudo, participaram mais de quinhentas pessoas, entre as quais foi possível observar uma redução de cerca de 45% na quantidade de participantes a serem vítimas de ataques de *Phishing* deste tipo.

Após a análise de ambas as metodologias, fica evidente a forte correlação entre a forma como os conteúdos são apresentados, e a retenção dos conteúdos por parte dos colaboradores. Para além disso, ambas as metodologias destacam-se por serem ótimas ferramentas de avaliação, uma vez que através dos seus resultados, é possível identificar quais são os colaboradores mais vulneráveis e que, por sua vez, precisam de ter um treino mais especializado para poderem aprender a reconhecer e evitar este tipo de ataques. Conclui-se também que as organizações que tiram proveito do treino comportamental devem focar-se em conteúdos mais atrativos e acima de tudo, direcionados para os colaboradores, em vez de oferecer conteúdos genéricos, que contribuem para a dimuição do desinteresse do público-alvo [17].

Capítulo 3

Contextualização da Plataforma

A *Cybersecurity Cloud* é uma plataforma *SaaS* e *Multi-Tenant* desenvolvida pela empresa EMVENCI. Esta plataforma tem como objetivo oferecer uma experiência integrada relacionada com a cibersegurança através de vários módulos.

3.1 Detalhes de Implementação

No contexto deste projeto, é importante salientar todos os detalhes técnicos relevantes à plataforma, nomeadamante quanto à sua implementação do *backend*. Esta foi escrita em Go (Golang), tirando proveito da arquitetura *Clean-Architecture* e REST, armazenando os seus dados através de uma base de dados MariaDB.

3.1.1 Plataforma *SaaS* e *Multi-Tenancy*

A plataforma segue o modelo *SaaS*, sendo as aplicações deste tipo conhecidas por oferecer soluções completas de *software* pagas conforme o seu uso. Os utilizadores alugam a aplicação, neste caso acedendo-a através de um navegador, sendo da responsabilidade do fornecedor gerir tanto o *hardware* como o *software*, garantindo sempre a disponibilidade e segurança dos dados dos utilizadores, como também da plataforma.[18]

Para além disso, segue também a arquitetura *Multi-Tenant*. Nesta arquitetura é possível que clientes distintos, ou neste caso *tenants*, possam utilizar a mesma aplicação simultaneamente, sem nunca saberem da presença dos restantes. Para isso, é utilizada uma única aplicação na qual todos os dados são armazenados na mesma base de dados, sendo estes dados separados logicamente pelo identificador único, que define cada *tenant* (Figura 3.1). [25]

3.1.2 Base de dados MariaDB

MariaDB é um sistema *open-source* de gestão de base de dados relacional. Este foi desenvolvido com base num *fork* do MySQL, tendo como objetivo melhorar alguns dos problemas existentes relacionados com a eficiência do seu predecessor. [2] Devido a isto, MariaDB acaba por ter uma alta compatibilidade com os sistemas que continuam a utilizar MySQL, facilitando também a sua

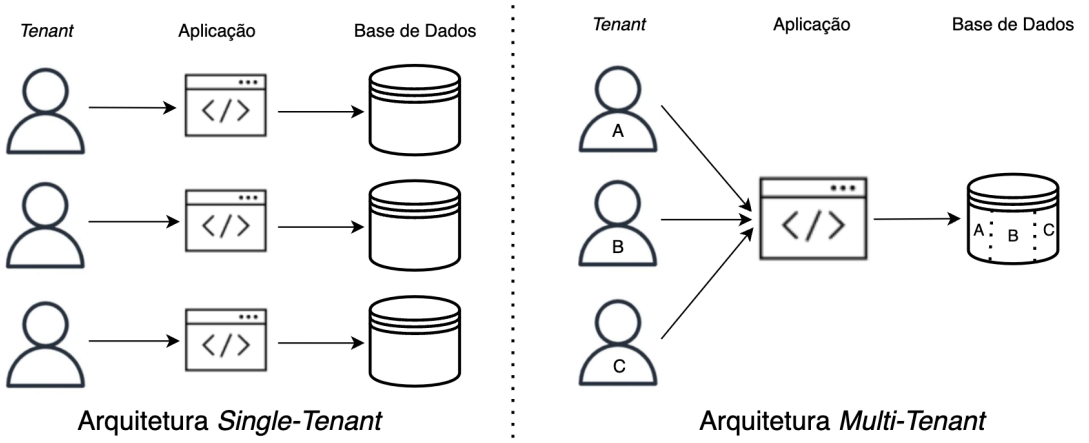

Figura 3.1: *Single-Tenant* vs *Multi-Tenant*

migração caso seja desejado. Para além disso, a MariaDB destaca-se pela sua velocidade e escalabilidade, tornando-se adequada para as diversas aplicações independentemente da sua dimensão, tendo sido utilizada como forma principal de armazenamento de dados para a plataforma *Cybersecurity Cloud*.

3.1.3 Golang

Para desenvolver todo o *backend* da plataforma *Cybersecurity Cloud* foi escolhida a linguagem Go. Esta, também mais conhecida como Golang, é uma linguagem de programação *open source* com um estilo sintático semelhante às linguagens C e C++. Foi desenvolvida pela *Google* em 2007 e lançada publicamente em 2009, com o objetivo de melhorar a produtividade dos programadores. [1]

Algumas das vantagens desta linguagem, para além da sua alta eficiência, são a sua simplicidade, o que facilita o processo de aprendizagem, e o facto de ser *statically-typed*, ou seja, o tipo das variáveis é definido em tempo de compilação, o que facilita a deteção precoce de erros. Para além disso, como a linguagem é *open source*, teve um aumento significativo na comunidade que a utiliza, o que consequentemente facilita todo o desenvolvimento. [4, 8]

3.1.4 *Clean-Architecture*

No que diz respeito à arquitetura da plataforma *Cybersecurity Cloud*, ela encontra-se de momento em migração para a *Clean-Architecture*. Desenvolvida por Robert Martin, esta foca-se na separação de responsabilidades, criando assim componentes independentes [16].

A *Clean-Architecture* baseia-se em dividir o sistema em múltiplas camadas, facilitando assim que o código seja mais testável, escalável e fácil de manter. Estas camadas, por sua vez, seguem uma hierarquia em que as camadas internas não podem ter dependências com as externas. Tais restrições acabam por tornar o código mais acessível, pois caso alguma peça do *software* precise

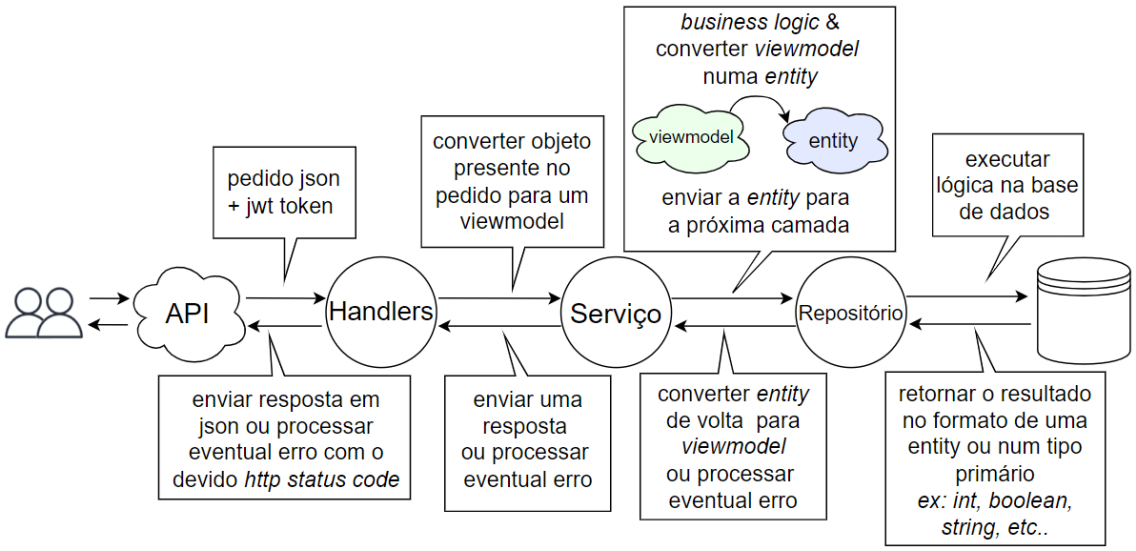

Figura 3.2: Exemplo de um pedido na arquitetura *Clean-Code*

de ser completamente remodelada, basta substituir a respetiva camada. [16]

No caso da plataforma, espera-se que, quando toda a migração do código esteja completa, a mesma esteja dividida nas seguintes camadas: repositórios, que realizam o acesso à base de dados através de *entities*; serviços, que acedem aos repositórios e são responsáveis por toda a *business logic*, enviando os dados (*viewmodels*) para a última camada; *handlers*, que processam todos os pedidos HTTP feitos à aplicação através de uma arquitetura REST, como pode ser observado no exemplo 3.2.

Espera-se então que, no fim da migração todo o código para esta arquitetura, toda a plataforma possa beneficiar das suas vantagens, contribuindo assim para uma base de código mais estável e fácil de manter.

3.1.5 Arquitetura REST

A arquitetura REST é uma abordagem bastante conhecida, utilizada para a criação de *Application Programming Interfaces* (APIs) flexíveis e de fácil compreensão, tendo sido então escolhida para a plataforma. Um dos benefícios mais conhecidos da REST é o facto de ser *stateless*, ou seja, cada pedido feito pelo cliente contém informação suficiente para que todo o processamento seja feito. Para além disso, a REST suporta operações HTTP, como *GET, POST, PUT* e *DELETE*, em que estas são utilizadas para realizar ações específicas sobre recursos da aplicação identificados pelo seu *URL*. [24]

É importante salientar que o uso desta arquitetura é bastante útil neste contexto, pois acaba por facilitar toda a comunicação entre a plataforma do utilizador (*frontend*) e o servidor onde todos os dados e processamento são realizados (*backend*).

3.1.6 Autenticação via Token JWT

Como método de autenticação a plataforma *Cybersecurity Cloud* utiliza *JSON Web Tokens* (JWT). Através do uso destes é possível ter *tokens* assinados associados à identidade de cada utilizador dentro da plataforma. Para isso, é gerado um *token* em formato *JSON* que contem as informações do utilizador, sendo este depois incluído no cabeçalho de todos os pedidos seguintes, como forma de garantir que a aplicação encontra-se a comunicar com o utilizador.

A vantagem da utilização deste método é que os *tokens* são assinados utilizando uma chave criptográfica. Através desta assinatura é então garantida a sua integridade, dificultando possíveis ataques em que um atacante tenta modificar os dados deste *tokens*. Isto acontece porque caso qualquer informação do *token* seja alterada após este ser assinado com uma chave criptográfica, o *token* e a respetiva assinatura ficam inválidos e não são aceites pela plataforma.

Mesmo assim esta propriedade dos *tokens* não invalida ataques em que um atacante capture o *token* de algum utilizador e utilize-o para aceder à plataforma. Para isso, o próprio *token* tem um tempo de vida definido. Através deste tempo de vida, que normalmente é relativamente curto, é possível reduzir o tempo que um atacante tem para fazer o seu ataque, visto que o *token* acaba por ficar inválido automáticamente ao fim de algum tempo, impedindo assim a sua reutilização pelo atacante.

3.2 Detalhes da Plataforma

No contexto desta dissertação, é também relevante detalhar alguns módulos presentes na plataforma, visto que serão alvo de estudo e melhoria. O módulo em questão tem como nome *Phishing Simulator*, sendo este, de entre todos os outros módulos disponibilizados pela plataforma o mais bem-sucedido.

O *Phishing Simulator* tem como propósito melhorar a resposta dos funcionários a ataques de *Phishing*. Para isso, este módulo simula cenários de ataques com as ameaças mais relevantes da atualidade, fornecendo aos colaboradores que falham *feedback* imediato, incluindo também a formação necessária através de conteúdos lúdicos, para que os colaboradores possam aprender com os seus erros.

O módulo tem o seguinte funcionamento: um administrador da plataforma, ao decidir que quer realizar um simulacro, (também apelidado de campanha), escolhe os alvos desejados (colaboradores da empresa), para que lhes seja simulado um ataque. Para isso escolhe também um *template* que representa o vetor de ataque, podendo este ser feito por diversos meios de comunicação (*Email*, *SMS*, *USB*, *NFC* e *QRCode*), além de também poder configurar como será o próprio aspeto do ataque. Para além disso, o administrador pode também testar a reação dos colaboradores perante uma plataforma forjada (*landing page*) durante a campanha, sendo esta para onde a vítima é redirecionada caso carregue no *link* presente na *template*.

Através da *landing page*, o administrador pode configurar, um cenário em que a plataforma para a qual o colaborador é redirecionado tem como objetivo aliciá-lo a inserir as suas credenciais

da empresa, ou simplesmente a carregar em algum tipo de *input*.

Uma vantagem que distingue este módulo é que permite que o administrador tenha também a opção de selecionar algum conteúdo educativo lúdico. Este, no formato de *PDF* ou vídeo, tem como propósito ser mostrado aos colaboradores quando eles falham à campanha.

Note-se que o conteúdo deve ser relacionado com o ataque realizado, para que o colaborador possa compreender onde errou e como se deve precaver para evitar cair novamente nesse erro. Não só isto, como também para complementar o momento de aprendizagem, o administrador pode adicionar um questionário após o conteúdo educativo, para verificar se o colaborador realmente prestou atenção ao conteúdo apresentado.

Todos os resultados do processo podem ser visíveis durante a campanha, para perceber o desempenho de cada colaborador.

Adicionalmente, quando o administrador decide terminar a campanha, a plataforma cria um relatório automático identificando os colaboradores que são considerados mais propícios a cair no tipo de ataque simulado, podendo estes valores serem influenciados pelas respostas submetidas nos questionários (caso tenha sido adicionado). Estes resultados influenciam como o colaborador é avaliado pela plataforma, podendo ficar sinalizado, indicando ao administrador de que representa um risco para a empresa devido à sua falta de conhecimento quanto à sua segurança *online*.

Num cenário ideal, após a análise destes resultados, um administrador deve aperceber-se de que o colaborador sinalizado necessita de uma aprendizagem mais aprofundada e especializada, dedicando-lhe uma maior atenção, o que pode não acontecer devido à falta de disponibilidade e qualificações do próprio administrador que gere a plataforma.

Capítulo 4

Análise dos Objetivos e Requisitos

A presente secção está omissa devido à confidencialidade inerente ao projeto.

Capítulo 5

Desenho da Solução

A presente secção está omissa devido à confidencialidade inerente ao projeto.

Capítulo 6

Implementação

A presente secção está omissa devido à confidencialidade inerente ao projeto.

Capítulo 7

Conclusão

Serve este capítulo como forma de apresentar uma visão geral de todo o trabalho realizado na EMVENCI durante a duração deste projeto. Para além disso são também apresentados aspetos que possam a vir a ser melhorados como forma de trabalho futuro para este projeto.

7.1 Trabalho Realizado

O presente trabalho focou-se na otimização e automatização do módulo de simulacros de *Phishing* da EMVENCI, fazendo este parte do projeto de conclusão do Mestrado em Engenharia Informática.

Após ser feita uma análise sobre os problemas presentes na formação de colaboradores quanto ao *Phishing* no mundo empresarial, foi possível desenvolver possíveis soluções e aplicá-las diretamente à plataforma levando ao seu melhoramento.

Identificou-se que o módulo atual de *Phishing* podia ser melhorado através da implementação de uma nova funcionalidade que permitisse a seleção de múltiplos cenários para um único simulacro, sendo que até ao momento só era possível selecionar um único cenário, o que poderia diminuir a sua eficácia. Tendo em conta que esta melhoria, apelidada de *Multi-Templates*, cumpriu com todos os requerimentos previamente definidos, é possível afirmar que a sua implementação foi bem-sucedida.

A maior parte deste projeto foi a implementação de uma nova forma de gerir os simulacros de *Phishing* através da sua automação. Esta automação permite que um administrador, ao responder a um questionário, faça com que a plataforme gere automaticamente múltiplas campanhas, geridas de forma autónoma. Toda esta automação tem como propósito tentar colmatar a falta de mão de obra e tempo que muitas vezes os administradores têm enquanto gerem a formação de milhares de colaboradores na sua empresa. Para isso, fez-se com que as campanhas criadas sejam lançadas automaticamente conforme as suas datas planeadas, e para além disso, caso existam colaboradores avaliados negativamente pela plataforma quanto aos seus conhecimentos, o próprio plano adapta-se ao atribuir a estes colaboradores campanhas adicionais, servindo assim como uma valiosa melhoria ao módulo atual de *Phishing* da EMVENCI.

Note-se que embora o desenvolvimento tenha sido feito sobre a plataforma já existente da EMVENCI, ambas as soluções foram desenvolvidas de raíz, tendo sido necessário planear meti-

culosamente toda a estrutura de ambas, desde a base de dados, até à interação do produto final com o cliente, dando-se como concluída toda a sua implementação visto que a ambas cumprem todos os requisitos desejados. Para além disso, todo o projeto foi rigorosmente testado, seja de forma manual ou através de testes unitários. Tudo encontra-se documentado de forma clara e direta, contribuindo assim para a continuidade e longevidade de todo o projeto.

Conclui-se assim, que após uma implementação bem-sucedida, este projeto poderá vir a ser uma grande vantagem na formação de colaboradores quanto ao *Phishing* no mundo empresarial.

7.2 Trabalho Futuro

Embora concluído o projeto, há sempre possíveis melhorias, como também ideias que venham a complementar o mesmo.

Começando com o *Multi-Template*, embora a implementação tenha sido bem-sucedida ela ainda pode sofrer algumas melhorias. De momento, a implementação do *Multi-Template* suporta os formatos *Email*, *SMS* e *Ransomware*, sendo que para este último apenas é submetido um único ficheiro comum a todos os cenários de ataque. Uma melhoria seria então permitir ao administrador selecionar múltiplos ficheiros. Obviamente esta ideia acaba por ter outros desafios, como processar múltiplos ficheiros de uma só vez pelo servidor entre muitos outros, tendo sido esta colocada como trabalho futuro. Outra melhoria seria a implementação do *Multi-Template* para os outros eventuais formatos de ataque presentes na plataforma, embora a forma como estes funcionam levanta outras questões.

Quanto às melhorias relativas à automação, todo o processo de responder ao questionário pode sempre ser otimizado, omitindo alguma das perguntas ao definir campos por *default* para cada *tenant*.

Toda a forma de como são gerados os relatórios sobre a automação também pode vir a ser bastante melhorada. De momento, cada campanha da automação gera um único relatório independente, não havendo então uma forma de correlacionar todos os dados destas campanhas num único relatório relevante a todo o planeamento de automação. Idealmente deveria haver uma secção contendo todos os dados das campanhas que tivessem sido executadas pelo planeamento até ao momento, mostrando assim todos os dados relevantes num único relatório e contribuindo assim para a pertinência deste módulo.

Para além disso, uma melhoria que deve ser investigada o quanto antes, seria como fazer com que em vez de ter um plano de automação a direcionar os simulacros para todos os colaboradores da plataforma, ter a opção de selecionar um grupo alvo mais específico. Esta melhoria embora pareça simples, acaba por ter um certo nível de complexidade visto que seria necessário criar grupos dinâmicos baseados em grupos já criados o que até ao momento ainda não existe na plataforma. Para além disso, tal como o *Multi-Templates*, a automação também pode ser melhorada ao utilizar mais do que os três formatos de campanhas até agora suportados, adicionando mais possibilidades para ao administrador.

Outra melhoria possível seria a otimização de todo o algoritmo responsável por gerar as cam-

panhas e de gestão do grupo de *high risk*, eventualmente até ao ponto de começar a utilizar algum tipo de *machine-learning*. Também todo o processo de gerar campanhas adicionais pode ser melhorado, fazendo com que as campanhas adicionais sejam geradas de forma aleatória em vez de basear-se numa campanha já gerada.

Finalmente, uma melhoria direcionada à plataforma seria tirar proveito de toda automação e lógica desenvolvida para que se venham a automatizar e melhorar outros módulos na plataforma, contribuindo assim cada vez mais, para uma boa experiência para a formação dos colaboradores quanto à área da cibersegurança.

Bibliografia

[1] *Go (linguagem de programação)*. Wikipedia, 2023.

[2] Jordana A. Mariadb vs mysql – key differences, pros and cons, and more. www.hostinger.com/tutorials/mariadb-vs-mysql, 2023. [Online - Accessed on 19-12-2023].

[3] Abdul Basit, Maham Zafar, Xuan Liu, Abdul Rehman Javed, Zunera Jalil, and Kashif Kifayat. A comprehensive survey of ai-enabled phishing attacks detection techniques. *Telecommunication Systems*, 76:139–154, 2021.

[4] Russ Cox. Go, open source, community. https://go.dev/blog/open-source, 2015. [Online - Accessed on 19-12-2023].

[5] Centro Nacional de Cibersegurança PORTUGAL. Csncs - glossário. https://www.cncs.gov.pt/pt/glossario/#linhasobservacao, 2023. [Online - Accessed on 12-12-2023].

[6] Centro Nacional de Cibersegurança PORTUGAL. Relatório cibersegurança em portugal. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf, 2023. [Online - Accessed on 12-12-2023].

[7] Field Effect. Overcoming the cybersecurity talent shortage in 2024. https://fieldeffect.com/blog/overcoming-the-cybersecurity-talent-shortage, 2023. [Online - Accessed on 17-12-2023].

[8] Julien Etienne. Why go: The benefits of golang. https://medium.com/@julienetienne/why-go-the-benefits-of-golang-6c39ea6cff7e, 2022. [Online - Accessed on 19-12-2023].

[9] Ryan Heartfield and George Loukas. A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks. *ACM Computing Surveys (CSUR)*, 48(3):1–39, 2015.

[10] Michael Hill. Cybersecurity workforce shortage reaches 4 million despite significant recruitment drive. https://www.csoonline.com/article/657598/cybersecurity-workforce-shortage-reaches-4-million-despite-

significant-recruitment-drive.html, 2023. [Online - Accessed on 17-12-2023].

[11] Matthew L Jensen, Michael Dinger, Ryan T Wright, and Jason Bennett Thatcher. Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems*, 34(2):597–626, 2017.

[12] Ponnurangam Kumaraguru, Justin Cranshaw, Alessandro Acquisti, Lorrie Cranor, Jason Hong, Mary Ann Blair, and Theodore Pham. School of phish: a real-world evaluation of anti-phishing training. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, pages 1–12, 2009.

[13] Ponnurangam Kumaraguru, Yong Rhee, Steve Sheng, Sharique Hasan, Alessandro Acquisti, Lorrie Faith Cranor, and Jason Hong. Getting users to pay attention to anti-phishing education: evaluation of retention and transfer. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 70–81, 2007.

[14] Ifigeneia Lella, Cosmin Ciobanu, Eleni Tsekmezoglou, Marianthi Theocharidou, Erika Magonara, Apostolos Malatras, Rossen Svetozarov Naydenov, et al. Enisa threat landscape 2023: July 2022 to june 2023. 2023.

[15] The Security Company (International) Limited. Quishing: Qr code based second wind for phishing attacks. https://www.linkedin.com/pulse/quishing-qr-code-based-second-wind-phishing-attacks-thesecurityco/, 2023. [Online - Accessed on 12-12-2023].

[16] Robert C Martin. Clean architecture, 2017.

[17] Steven McElwee, George Murphy, and Paul Shelton. Influencing outcomes and behaviors in simulated phishing exercises. In *SoutheastCon 2018*, pages 1–6. IEEE, 2018.

[18] Microsoft. O que é saas? https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-is-saas, 2023. [Online - Accessed on 19-12-2023].

[19] Slash Next. The state of phishing 2023. https://slashnext.com/state-of-phishing-2023/, 2023. [Online - Accessed on 5-3-2024].

[20] Nivedita James Palatty. 81 phishing attack statistics 2023: The ultimate insight. https://www.getastra.com/blog/security-audit/phishing-attack-statistics/, 2023. [Online - Accessed on 12-12-2023].

[21] Benjamin Reinheimer, Lukas Aldag, Peter Mayer, Mattia Mossano, Reyhan Duezguen, Bettina Lofthouse, Tatiana Von Landesberger, and Melanie Volkamer. An investigation of phishing awareness and education over time: When and how to best remind users. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 259–284, 2020.

[22] Calif Sausalito. Cybersecurity jobs report: 3.5 million unfilled positions in 2025. https://cybersecurityventures.com/jobs/, 2023. [Online - Accessed on 6-3-2024].

[23] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99, 2007.

[24] Codecademy Team. What is rest? https://www.codecademy.com/article/what-is-rest. [Online - Accessed on 19-12-2023].

[25] TechTarget. Multitenancy. https://www.techtarget.com/whatis/definition/multi-tenancy, 2023. [Online - Accessed on 18-12-2023].

[26] TRENDMicro. Quais são os diferentes tipos de phishing? https://www.trendmicro.com/pt_br/what-is/phishing/types-of-phishing.html, 2023. [Online - Accessed on 7-12-2023].

[27] Alma Whitten and JD Tygar. Whyjohnnycan'tencrypt: Ausabilityevaluationo fpgp 5. 0. 1999.

[28] Wikipedia. Engenharia social (segurança) — Wikipedia, the free encyclopedia. http://pt.wikipedia.org/w/index.php?title=Engenharia%20social%20(seguran%C3%A7a)&oldid=67068421, 2024. [Online; Accessed 10-April-2024].

Apêndice A

Algoritmo

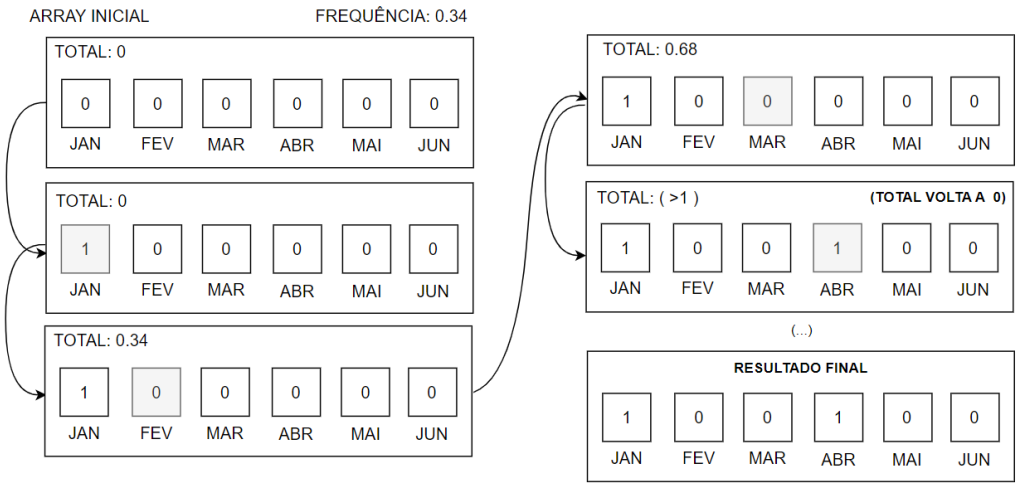

Figura A.1: Representação visual do algoritmo de geração do número de campanhas por mês, para a duração de seis meses com uma frequência de 0.34 (uma campanha a cada três meses)

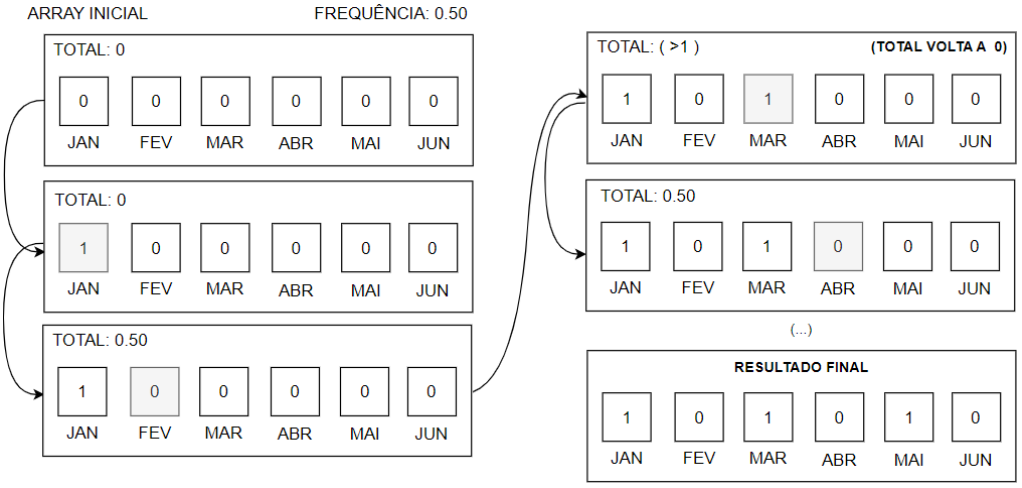

Figura A.2: Representação visual do algoritmo de geração do númeor de campanhas por mês, para a duração de seis meses com uma frequência de 0.50 (uma campanha a cada dois meses)