ESCOLA DE GUERRA NAVAL

CC(T) CRISTIANE DA SILVA RODRIGUES PEREIRA

PROTEÇÃO CIBERNÉTICA:
Uma proposta para aprimorar a segurança dos sistemas digitais da Marinha do Brasil

Rio de Janeiro

2024

CC(T) CRISTIANE DA SILVA RODRIGUES PEREIRA

PROTEÇÃO CIBERNÉTICA:
Uma proposta para aprimorar a segurança dos sistemas digitais da Marinha do Brasil

Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior.

Orientador: CC Bruno Roberto de Gouvêa Rodrigues Pimenta

Rio de Janeiro

Escola de Guerra Naval

2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

gov.br
Documento assinado digitalmente
CRISTIANE DA SILVA RODRIGUES PEREIRA
Data: 16/11/2024 13:59:41-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

Agradeço primeiramente a Deus, por estar sempre ao meu lado e por ter me sustentado até este momento da minha jornada.

Ao meu marido Carlos José e aos meus filhos Carlos Guilherme e Carlos Gustavo, pelo amor, apoio e compreensão incondicionais.

Aos meus pais, Rosa e Sergio, pela educação e oportunidades que foram fundamentais para o meu desenvolvimento pessoal e profissional.

Aos meus chefes, Capitão de Mar e Guerra (T) Maria Rezende e Capitão de Fragata Waldomiro que me apoiaram para que eu conseguisse cumprir com êxito este curso.

Aos amigos e companheiros de trabalho, Capitão de Fragata (T) Patrícia Rocha, Capitão de Corveta (T) Tânia Siqueira e Capitão de Corveta (T) Lyssandra, que tanto me ajudaram ao longo deste trabalho e de todo o curso.

À equipe responsável pela disciplina de Metodologia de Pesquisa, que sempre esteve disponível e preocupada em transmitir todos os conhecimentos necessários para realização deste trabalho.

Ao meu orientador, cujas observações foram fundamentais para a melhoria gradativa e a conclusão desta monografia.

“A tarefa não é tanto ver aquilo que ninguém viu, mas pensar o que ninguém ainda pensou sobre aquilo que todo mundo vê.”

Arthur Schopenhauer

RESUMO

O número de ataques cibernéticos aos sistemas digitais de instituições governamentais e privadas está em crescimento. Este estudo visou apresentar os principais ataques e vulnerabilidades de *software* que podem acometer esses sistemas digitais. Além disso, explorou a estrutura de defesa cibernética da Marinha e suas operações cibernéticas, e os processos de desenvolvimento e homologação de sistemas digitais. Para atingir o objetivo deste trabalho, foi utilizado como método de coleta de dados, a pesquisa bibliográfica e entrevistas. A partir da análise dos dados foi possível perceber que exercícios de Guerra Cibernética são realizados para fortalecer as competências da Marinha no enfrentamento de ameaças cibernéticas. Como também, que o processo de desenvolvimento de sistemas não adota metodologias de desenvolvimento seguro, podendo assim, comprometer a Proteção Cibernética da rede da Marinha do Brasil. Portanto, este trabalho propõe uma solução para aprimorar os processos de desenvolvimento e homologação dos sistemas digitais da Marinha do Brasil, visando elevar a segurança desses sistemas e, por conseguinte, reforçar a Proteção Cibernética da Marinha. Por fim, a implementação dessa solução precisa ser realizada pela Diretoria de Comunicações e Tecnologia da Informação da Marinha, de forma gradual e centralizada, contando com o apoio das Organizações Militares desenvolvedoras de sistemas digitais.

Palavras-chave: Operações Cibernéticas. Proteção Cibernética. Segurança da Informação. Sistemas Digitais. Desenvolvimento de Sistemas.

ABSTRACT

Cyber protection:
A proposal to improve the security of the Brazilian Navy’s digital systems

The number of cyber attacks on the digital systems of government and private institutions is growing. This study aimed to present the main software attacks and vulnerabilities that can affect these digital systems. Furthermore, it explored the Navy's cyber defense structure and its cyber operations, and the development and approval processes of digital systems. To achieve the objective of this work, bibliographic research and interviews were used as data collection methods. From the data analysis, it was possible to see that Cyber War exercises are carried out to strengthen the Navy's skills in facing cyber threats. Also, the system development process does not adopt secure development methodologies, thus potentially compromising the Cyber Protection of the Brazilian Navy network. Therefore, this work proposes a solution to improve the development and approval processes of the Brazilian Navy's digital systems, aiming to increase the security of these systems and, therefore, reinforce the Navy's Cyber Protection. Finally, the implementation of this solution needs to be carried out by the Navy's Directorate of Communications and Information Technology, in a gradual and centralized manner, with the support of Military Organizations that develop digital systems.

Keywords: Cyber Operations. Cyber Protection. Information Security. Digital Systems. Systems Development.

SUMÁRIO

1 INTRODUÇÃO

Com o avanço dos Sistemas Digitais (SD) e principalmente da Internet, as pessoas mostram-se cada vez mais dependentes de sistemas on-line para realizarem tarefas do cotidiano como fazer compras, pagar contas ou estudar. Nas atividades da Marinha, observa-se o mesmo, com muitos sistemas automatizando importantes atribuições da instituição, como é o caso do Sistema de Informações sobre o Tráfego Marítimo (SISTRAM) e o Sistema de Identificação e Acompanhamento de Navios a Longa Distância (LRIT).

O desenvolvimento de SD, visando automatizar tarefas que são realizadas manualmente pelas pessoas, permite maior agilidade e assertividade na execução dos processos de uma organização. Porém, muitas vezes a necessidade de entrega rápida de um sistema e/ou a falta de um especialista da área de segurança faz com que as organizações não utilizem boas práticas de segurança durante o desenvolvimento de um *software*, deixando-o vulnerável a ataques cibernéticos.

O aumento do uso da tecnologia e de sua dependência, em conjunto com as vulnerabilidades dos SD, culminou no crescimento do número de ataques cibernéticos. Em 2022, o Brasil foi o segundo país mais afetado da América Latina, registrando 103,16 bilhões de tentativas de ataques cibernéticos, um aumento de 16% em relação ao ano anterior, quando foram registradas 88,5 bilhões de tentativas, conforme levantamento divulgado pela empresa de soluções de cibersegurança Fortinet (Febraban, 2023). Nesse cenário, nos últimos três meses, foram registradas 1.962.522 tentativas de ataque aos SD da Marinha do Brasil (MB) acessíveis pela Internet, o que representa 97% do total de tentativas, conforme detalhado no Apêndice A.

Essa questão é tão preocupante que o Fórum Econômico Mundial considera os ciberataques como o quinto risco com maior probabilidade de apresentar uma crise material em escala global em 2024 (World Economic Forum, 2024). Cabendo destacar que, quando uma tentativa de ataque a um SD é bem-sucedida, toda a rede pode vir a ser comprometida.

Novas vulnerabilidades de segurança são descobertas diariamente e a grande maioria dos ataques cibernéticos exploram as falhas de segurança dos SD

(Aslan *et al*., 2023). Por isso, os sistemas, incluindo os da MB, devem ser atualizados continuamente a fim de evitar que esses ataques tenham sucesso e venham causar a indisponibilidade dos serviços e a divulgação de dados sensíveis da Força e de seus militares. Portanto, o maior desafio enfrentado pelos desenvolvedores de sistemas da MB é implementar sistemas utilizando as melhores práticas de segurança, garantindo que as tecnologias utilizadas estejam sempre atualizadas e sem vulnerabilidades.

Diante da motivação apresentada, o objetivo principal desta monografia é propor uma solução que aprimore a segurança dos SD da MB ainda durante a fase de desenvolvimento desses sistemas, visando aumentar a segurança da Rede de Comunicações Integradas da Marinha (RECIM) contra ataques cibernéticos. Para tanto, será necessário compreender os processos de desenvolvimento e homologação de SD, para identificar as oportunidades de aprimoramento. Nesse ínterim, os objetivos específicos desse estudo são: discriminar as ameaças e as vulnerabilidades cibernéticas, para compreender como os ataques cibernéticos podem comprometer os SD; descrever a estrutura de defesa cibernética da MB, incluindo suas limitações, além das operações cibernéticas que são realizadas pela a MB com o intuito de aprimorar as suas capacidades de Defesa Cibernética (DCiber) e Proteção Cibernética (PtçCiber).

O uso de metodologia de desenvolvimento seguro é amplamente adotado por muitas empresas há algum tempo, mas a sua adoção pela MB ainda não foi realizada em virtude de alguns problemas como a falta de uniformidade no processo de desenvolvimento, que são descentralizados, bem como a dificuldade de manutenir sistemas legados[1], o que é uma tarefa complexa.

Desta forma, esta pesquisa visa apresentar uma proposta de reestruturação dos processos de desenvolvimento e homologação de SD, com o intuito de aprimorar a segurança dos SD durante a fase de desenvolvimento, visando aumentar a proteção da RECIM contra ataques cibernéticos.

A pesquisa consiste na análise dos atuais processos de desenvolvimento e homologação de SD na MB, com o intuito de recomendar a adoção de melhores práticas de segurança da informação nesses processos, para reduzir as

1 Sistemas que utilizam tecnologias obsoletas.

vulnerabilidades de segurança dos SD. Portanto, o resultado desta pesquisa é de grande relevância para a MB, tendo em vista que identifica uma nova forma de conduzir os processos de desenvolvimento e de homologação de sistemas na MB, com foco na segurança cibernética.

Quanto à metodologia, este trabalho foi realizado com base na técnica de pesquisa de documentação indireta, sendo utilizada a pesquisa bibliográfica seletiva em fontes abertas como principal forma de coleta de dados, além da realização de entrevistas com Oficiais da MB responsáveis pela homologação de SD e pelo monitoramento de incidentes cibernéticos na MB. A pesquisa bibliográfica foi realizada nas páginas de internet https://scholar.google.com e www.repositorio.mar.mil.br, tendo sido utilizadas as palavras chaves "*software vulnerability*", "*software development*", "*cyberattack*" e "guerra cibernética". Adicionalmente, foram considerados apenas os retornos a partir de 2011, em língua portuguesa e inglesa.

Além das fontes mencionadas, foram utilizadas as normas do Estado-Maior da Armada (EMA), da Diretoria-Geral do Material da Marinha (DGMM) e da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), tais como: EMA-305, EMA-419, DGMM-0540, DCTIMARINST 30-17, DCTIMARINST 33-06B e DCTIMBOTEC 30/002/2023.

Esta monografia está organizada em cinco capítulos, incluindo a Introdução. No Capítulo 2, apresentam-se as principais ameaças e vulnerabilidades cibernéticas que podem comprometer a disponibilidade e a segurança dos serviços de uma organização. No Capítulo 3, apresentam-se conceitos sobre a estrutura de defesa cibernética da MB e suas limitações, além das operações cibernéticas que já foram realizadas pela MB. No Capítulo 4, apresenta-se a questão de pequisa e o resultado da análise com a respectiva discussão. Por último, no Capítulo 5, apresenta-se a contribuição deste estudo, as limitações e os possíveis trabalhos futuros relacionados ao assunto.

2 ATAQUES, AMEAÇAS E VULNERABILIDADES CIBERNÉTICAS

A Guerra Cibernética (GCiber) abrange tanto o uso ofensivo quanto defensivo de informações e Sistemas de Informação, visando negar, explorar, corromper, degradar ou destruir as capacidades de Comando e Controle (C2) do adversário. Este processo ocorre dentro do contexto de planejamento militar em níveis operacionais ou táticos, assim como durante a condução de operações militares (Brasil, 2021a).

Além disso, a GCiber desempenha um papel cada vez mais relevante nas operações militares modernas, sendo empregada para uma ampla gama de propósitos, desde a obtenção de informações e inteligência até ataques contra Infraestruturas Críticas (IC)[2]. Nesse contexto, compreender os métodos e táticas utilizados nos ataques cibernéticos é fundamental para o desenvolvimento de estratégias eficazes de defesa cibernética.

As ameaças e vulnerabilidades cibernéticas são questões críticas no mundo digital de hoje. A segurança da informação e a segurança cibernética são áreas intimamente relacionadas que lidam com a proteção dos dados, sistemas e infraestrutura digital contra ameaças e vulnerabilidades cibernéticas.

A Segurança da Informação refere-se ao conjunto de práticas, políticas, procedimentos e tecnologias, projetadas para garantir os requisitos básicos como a disponibilidade, a integridade, a confidencialidade e a autenticidade, da informação, dos dados e dos sistemas de uma organização. Esses requisitos são conhecidos pelo acrônimo DICA. Já a Segurança Cibernética é uma parte essencial da segurança da informação que busca proteger ativos de Tecnologia da Informação e Comunicações (TIC), sistemas, IC e tudo que esteja no domínio cibernético (Brasil, 2021).

A disponibilidade visa assegurar que as informações estejam disponíveis quando necessárias para pessoas autorizadas, portanto esse requisito envolve redundância, *backup* de dados e tolerância a falhas. A integridade tem o objetivo de garantir que as informações não sejam corrompidas ou alteradas de forma não autorizada, e para que isso aconteça, se necessário incluir o controle de versões,

2 “Instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade “ (Brasil, 2021a, p.98).

assinaturas digitais e *hash*[3]. A confidencialidade busca garantir que apenas pessoas autorizadas tenham acesso às informações confidenciais, e para atender esse requisito, há a necessidade do uso da criptografia, de políticas de compartilhamento de informações e de controle de acesso às informações. Por último, a autenticidade visa assegurar que os dados, sistemas, usuários ou entidades envolvidas em uma transação ou comunicação são legítimos e não foram alterados ou falsificados. Garantir a autenticidade é importante para proteger a integridade e manter a confiança nos sistemas de informação.

2.1 HISTÓRICO DE ATAQUES CIBERNÉTICOS

O artefato malicioso *Stuxnet* tornou-se um marco na história da cibersegurança. Projetado para operar de forma modular e em etapas, ele inicialmente realiza uma infecção geral, espalhando-se de um computador para outro até localizar seu alvo específico. O objetivo do *Stuxnet* foi de atacar somente quando encontrar sistemas industriais específicos, como os controladores lógicos programáveis (PLCs) da central de enriquecimento nuclear do Irã. O *Stuxnet* modificou as configurações que controlam a velocidade das centrífugas, resultando em seu mau funcionamento (Denning, 2012).

Cabe ressaltar que o *Stuxnet* explorou várias vulnerabilidades do sistema operacional *Windows*, especificamente as falhas no serviço de impressão e na execução remota de código. Essas vulnerabilidades permitiram que o Stuxnet se espalhasse de forma rápida e silenciosa por meio de redes de computadores (Correia; Rigues, 2021). Esse ataque levou à paralisação do programa nuclear iraniano por vários anos.

DarkSeoul é o nome dado a uma série de ataques cibernéticos que afetaram a Coreia do Sul. Esses ataques iniciaram em 2013 e visavam principalmente entidades governamentais e instituições financeiras, causando danos significativos aos sistemas de Tecnologia da Informação (TI). Embora não sejam exclusivamente focados em operações militares, os ataques tiveram impactos que afetaram a capacidade de resposta e a segurança nacional sul-coreana, incluindo aspectos

3 Função matemática que transforma uma quantidade de dados em uma sequência de caracteres alfanuméricos de comprimento fixo.

relacionados à defesa. Pesquisadores e o governo sul-coreano chegaram à conclusão de que os ataques foram provenientes da Coreia do Norte e representaram um ataque direcionado para a Coreia do Sul. A capacidade dos invasores de distribuir sua carga destrutiva para dezenas de milhares de sistemas vítimas ocorreu devido ao acesso ao gerenciamento de patches[4] do *software* AhnLab[5]. Este acesso, utilizando credenciais legítimas roubadas, deu aos atacantes a capacidade de instalar o *software* malicioso (Martin, 2015).

Portanto, o sucesso de um ataque cibernético a um sistema digital de uma Força Armada pode ter consequências devastadoras e de larga escala, comprometendo a segurança nacional e a integridade da defesa. Dados sensíveis sobre estratégias militares, operações e pessoal podem ser acessados e manipulados, potencialmente expondo planos táticos e secretos a adversários. A resposta a tais ataques exige uma coordenação intensa e uma recuperação rápida para restaurar a segurança e a funcionalidade das operações militares.

2.2 TIPOS DE AMEAÇAS CIBERNÉTICAS

A compreensão das vulnerabilidades que acometem as aplicações *web* é crucial para entender como os ataques cibernéticos podem ser perpetrados. As ameaças exploram vulnerabilidades, assim como os ataques são as ameaças que foram concretizadas e, se bem-sucedidos, podem causar a violação de, pelo menos, um dos requisitos básicos da Segurança da Informação.

Há diversos tipos de ameaças no Espaço Cibernético[6] (ECiber), desde o surgimento da Internet. Para este estudo, são abordados os tipos mais comuns de ameaças cibernéticas, especialmente aquelas direcionadas à exploração das vulnerabilidades em aplicações *web*.

---

4 Os *patches* servem para corrigir falhas de segurança ou outros bugs que existem em uma versão anterior do *software*.

5 “Empresa de *software* sul-coreana que fornece soluções antivírus para terminais e redes” (Zacks, 2024, n.p).

6 “Espaço virtual, composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantam a interconexão de dispositivos de Tecnologia da Informação e Comunicações (TIC)” (Brasil, 2021a, p.96).

2.2.1 *Structured Query Language (*SQL) *Injection*

Geralmente, os aplicativos *web* interagem com Sistemas de Gerenciamento de Banco de Dados (SGBDs). Para tanto, é utilizada uma linguagem de programação estruturada, conhecida como SQL para inserir, atualizar, excluir ou consultar dados armazenados nos bancos de dados.

O ataque de SQL *Injection* é uma técnica de exploração de vulnerabilidades em SGBDs, em que um invasor insere instruções SQL maliciosas em campos de entrada de dados de um aplicativo, com o objetivo de manipular o banco de dados de forma não autorizada.

Quando os desenvolvedores não implementam a devida validação e sanitização das entradas de dados do usuário, um invasor pode inserir comandos SQL maliciosos que são executados pelo SGBD. Adicionalmente, o atacante envia uma consulta malformada no texto de entrada. Esta consulta é elaborada de tal maneira que, mesmo com o uso de credenciais de usuário incorretas, resulta em uma consulta verdadeira, permitindo assim que o atacante obtenha acesso ao banco de dados (Bukirari; Dar Iqbal, 2018; Patel, 2019). A principal razão para o ataque é a não verificação dos dados de entrada antes da utilização desses dados para realizar a consulta de pesquisa (Goutam; Tiwari, 2019).

Os ataques de SQL *Injection* podem ser devastadores, pois permitem que os invasores acessem, modifiquem ou excluam dados sensíveis, executem operações afetas à administração do banco de dados e até mesmo comprometam todo o sistema onde o banco de dados está hospedado. É possível evitar esse tipo de ataque, para isso é essencial que os desenvolvedores de sistemas implementem práticas de segurança, como o uso de consultas parametrizadas que evitam a concatenação de *strings* para formar consultas SQL. Ademais, é importante realizar a validação e a sanitização de todas as entradas de dados do usuário.

2.2.2 *Cross Site Scripting* (XSS)

XSS é um tipo de ataque de injeção de código malicioso em sistemas *web*. Os dados inseridos pelo usuário não são devidamente validados antes de serem integrados às páginas *web*, tornando possível sua exibição para outros usuários, o que pode resultar em consequências prejudiciais. O invasor injeta *scripts*[7] maliciosos na página *web*, podendo resultar no controle da conta do usuário, roubo de sessão ou redirecionamento para o site do invasor quando o usuário processa o *script* (Weamie, 2022). O ataque XSS pode ser desencadeado em qualquer site suscetível, independentemente da linguagem de programação em que foi escrito. No entanto, é mais comumente encontrado em aplicações desenvolvidas em *JavaScript.*

Existem diferentes tipos de XSS, persistente e não persistente. O XSS persistente envolve o armazenamento dos dados maliciosos no servidor da aplicação, enquanto que o XSS não persistente, também chamado de XSS refletido, implica a injeção temporária de dados maliciosos na página *web* (Weamie, 2022).

Para prevenir ataques XSS, é fundamental adotar práticas seguras de codificação. Isso inclui filtrar e validar as entradas do usuário, utilizar bibliotecas atualizadas para tratar o código da aplicação e implementar cabeçalhos de segurança HTTP[8], como a C*ontent Security Policy* (CSP).

2.2.3. *Cross-Site Request Forgery* (CSRF)

CSRF é um tipo de ataque cibernético em sistemas *web* em que um invasor engana um usuário legítimo a executar ações indesejadas em um aplicativo *web* no qual ele está autenticado. Isso é feito enviando uma solicitação HTTP maliciosa de um site diferente, enquanto o usuário está autenticado em outro site.

Este tipo de ataque força o navegador da vítima a executar uma ação indesejada a partir de um usuário em quem a aplicação *web* confia e sem a interação do usuário, explorando a confiança de um site no navegador do usuário (Siddiqui; Verma, 2011). Por exemplo, um atacante pode criar um *link* ou um formulário em um site malicioso, que envia uma solicitação para modificar as

7 Conjunto de comandos que devem ser executados por um recurso computacional.

8 “HTTP é a sigla para *Hypertext Transfer Protocol*, ou Protocolo de Transferência de Hipertexto. Esse é o principal protocolo responsável pela transferência de dados na Internet, criando as bases necessárias para a conexão entre um cliente e um servidor”(Santana, 2023).

configurações da conta de um usuário em um site legítimo, onde o usuário já está autenticado. Se o usuário clicar no *link* ou enviar o formulário, a solicitação será executada utilizando as credenciais do usuário legítimo, com isso, a modificação indesejada ocorrerá sem o conhecimento do usuário.

Para prevenir o ataque de CSRF, as aplicações *web* podem utilizar *tokens* anti-CSRF, também conhecidos como *tokens synchronizer*, para verificar se as solicitações são legítimas. Esses *tokens* são gerados pelo servidor da aplicação e incluídos nas páginas da *web* como campos ocultos em formulários ou como cabeçalhos HTTP. Portanto, quando o usuário envia uma solicitação, o servidor verifica se o *token* enviado corresponde ao esperado, impedindo assim solicitações CSRF maliciosas. Entretanto, o uso desses *tokens* precisa ser configurado pelo desenvolvedor do sistema.

2.3 VULNERABILIDADES CIBERNÉTICAS

A *Open Web Application Security Project* (OWASP) é uma comunidade internacional aberta dedicada a fornecer recursos e informações para ajudar na melhoria da segurança das aplicações *web* (Owasp, 2021). A OWASP desenvolveu uma série de recursos que descrevem as vulnerabilidades mais comuns existentes em vários sistemas, incluindo aplicações *web*, API[9] (*Application Programming Interface*), dispositivos móveis e entre outros. Um dos recursos mais conhecido é o OWASP Top 10, que enumera as dez vulnerabilidades mais críticas e frequentemente encontradas em aplicativos *web* em produção. Este documento é produzido considerando a frequência das vulnerabilidades, representando a porcentagem de aplicativos afetados por cada uma delas. Além disso, apresenta práticas recomendadas para prevenir essas vulnerabilidades, acompanhado de descrições de como elas podem ser exploradas. A versão mais recente do OWASP Top 10 foi lançada em 2021, sendo atualizada com base em dados de testes de segurança e pesquisas realizadas com profissionais do setor.

É importante destacar que as instituições enfrentam um desafio significativo

9 Interface de Programa de Aplicação (API) é um código que permite que duas aplicações de *software* se comuniquem entre si.

para proteger os seus sistemas contra as vulnerabilidades conhecidas como *zero day*. Uma vulnerabilidade *zero day* é uma falha de segurança em *software*, *hardware* ou *firmware*[10] que é desconhecida pelo fabricante do produto ou pelos desenvolvedores de *software* e, portanto, não tem uma solução ou *patch* disponível para correção da vulnerabilidade. Como não há solução imediata disponível, os sistemas afetados podem estar expostos a ataques maliciosos até que uma correção seja desenvolvida e implementada. Essas vulnerabilidades são valorizadas pelos atacantes e podem ser exploradas para realizar ataques cibernéticos graves.

Adicionalmente, as ameaças cibernéticas tornam-se viáveis quando os atacantes identificam falhas de segurança nos sistemas, como por exemplo, erros de programação do código-fonte, falta do uso de criptografia, ausência de aplicação de *patches* para correção e atualização de *software* e falta de validação de dados de entrada do sistema.

Cabe ressaltar que diferentes sistemas possuem vulnerabilidades distintas e que essas falhas estão em constante mudança. À medida que algumas vulnerabilidades são corrigidas, novas podem surgir. Antes de realizar um ataque cibernético, o atacante identifica essas fragilidades utilizando ferramentas especializadas em varredura de vulnerabilidades e, posteriormente, explora essas falhas encontradas. Assim, é essencial um esforço contínuo para identificar, avaliar e mitigar riscos de segurança nos sistemas.

Esse estudo ressalta a importância de proteger principalmente os SD hospedados na DMZ[11] (zona desmilitarizada) do Centro de Dados da Marinha do Brasil (CD-MB), pois estes estão disponíveis na Internet para serem acessados por qualquer pessoa. Como exemplo de SD hospedados na DMZ destacam-se o SISTRAM e o LRIT.

O SD SISTRAM monitora o tráfego de navios e embarcações na região de busca e salvamento brasileira utilizando informações de navegação padronizadas. Esse acompanhamento auxilia as operações de socorro, garantindo o uso eficiente e eficaz dos recursos de busca e salvamento para a proteção da vida humana. Por

10 “Um tipo de *software* que está embutido em um dispositivo eletrônico, sendo responsável por controlar e gerenciar o hardware desse dispositivo” (Oliveira, 2023, n.p).

11 Sub-rede posicionada entre a internet pública e as redes privadas, que permite a exposição controlada de serviços externos a redes não confiáveis, oferecendo uma camada adicional de segurança para proteger dados confidenciais armazenados nas redes internas (Fortinet, [s.d.]).

outro lado, o LRIT monitora a movimentação de navios mercantes de bandeira brasileira, sujeitos à Convenção Internacional para Salvaguarda da Vida Humana no Mar.

A presença de vulnerabilidades em sistemas localizados na DMZ podem servir como uma porta de entrada para possíveis atacantes. Se esses sistemas apresentarem falhas de segurança, elas podem ser exploradas para obter acesso à rede interna da instituição. Uma vez dentro da rede, o invasor pode acessar os SD hospedados na intranet e comprometer a sua integridade por meio de ataques como SQL injection e XSS. Esses ataques podem resultar no acesso e na manipulação de dados sensíveis, como informações sobre ilícitos praticados no mar territorial brasileiro ou no posicionamento dos navios de guerra da MB. Portanto, garantir a segurança dos sistemas na DMZ é crucial para proteger a integridade e a confidencialidade das informações da MB.

Nesta seção foram apresentados conceitos essenciais para a compreensão desta pesquisa, abrangendo as principais características dos ataques cibernéticos ocorridos durante operações militares, os tipos mais comuns de ataques cibernéticos às aplicações *web* e as vulnerabilidades de segurança exploradas por tais ataques. É importante destacar que as vulnerabilidades de segurança permeiam tanto os dispositivos de TIC quanto os SD e, devido à crescente incidência do comprometimento de sistemas e sites organizacionais, a mitigação dessas vulnerabilidades de segurança surge como uma grande preocupação para as organizações.

No próximo capítulo, serão abordados conceitos sobre a estrutura de defesa cibernética da MB, os exercícios de GCiber que são realizados pela MB para aprimorar sua capacidade de defesa cibernética e as limitações da defesa cibernética, que dentre elas, inclui as vulnerabilidades nos sistemas de informação.

3 DEFESA CIBERNÉTICA E LIMITAÇÕES

A segurança no ECiber tem se tornado cada vez mais importante na política de defesa de muitos países, incluindo o Brasil. Em virtude do avanço da tecnologia e

da crescente presença dos SD Administrativos[12] e dos SD Operativos[13] nas Organizações Militares (OM) da MB, os ataques cibernéticos representam uma ameaça significativa.

No contexto da Capacidade Nacional de Defesa da Proteção, na Estratégia Nacional de Defesa (END), destaca-se “garantir a soberania” como o objetivo nacional mais relevante (Brasil, 2020c). A END define como setores estratégicos da Defesa: o nuclear, o cibernético e o espacial. Nessa abordagem, a END faz sua primeira referência ao ECiber, reconhecendo-o como uma área crítica que requer proteção junto ao território nacional, às Águas Jurisdicionais Brasileiras, ao espaço aéreo sobrejacente e ao espaço exterior. Além disso, a segurança cibernética também desempenha um papel crucial na proteção dos interesses nacionais, na garantia da soberania digital e na preservação da estabilidade e da segurança internacional.

Em 2012, o Ministério da Defesa (MD) estabeleceu a Política Cibernética de Defesa (Brasil, 2012), visando orientar as atividades de DCiber no âmbito estratégico, assim como a GCiber nos níveis operacional e tático, para alcançar seus objetivos. Um dos principais objetivos desta política é desenvolver e manter atualizada a doutrina de emprego do Setor Cibernético. Em consonância com essa política, o MD aprovou, em 2014, a Doutrina Militar de Defesa Cibernética (Brasil, 2023b) que reconhece dois campos distintos a partir da END: a Segurança Cibernética, sob a responsabilidade da Presidência da República, e a DCiber, a cargo do MD por meio das Forças Armadas.

A DCiber engloba uma série de medidas executadas no ambiente digital, dentro de um plano estratégico nacional, coordenado pelo MD. Seu propósito é resguardar os recursos de informações vitais para a segurança nacional, além de adquirir informações para a elaboração de inteligência, visando assegurar uma posição de superioridade nos sistemas de informação do adversário.

A DCiber engloba uma série de medidas executadas no ambiente digital, dentro de um plano estratégico nacional, coordenado pelo MD. Seu propósito é resguardar os recursos de informações vitais para a segurança nacional, bem como proteger os SD contra ameaças cibernéticas, além de adquirir informações para a

12 Sistemas de informação que apoiam as atividades administrativas da MB (Brasil, 2019a).
13 Sistemas de informação empregados em operações navais ou em seu benefício (Brasil, 2019a).

elaboração de inteligência. O objetivo é assegurar uma posição de superioridade nos sistemas de informação do adversário, garantindo a integridade e a eficácia das operações e das comunicações digitais essenciais para a defesa nacional.

3.1 ESTRUTURA DE DEFESA CIBERNÉTICA NACIONAL

Uma das diretrizes fundamentais da Política Cibernética de Defesa aborda a concepção e implementação do Sistema Militar de Defesa Cibernética (SMDC) (Brasil, 2012). O SMDC, estabelecido em novembro de 2020, pode ser definido como "um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do ECiber pela Defesa Nacional" (Brasil, 2020d, p.12). O órgão central do SMDC é o Comando de Defesa Cibernética (ComDCiber), comando operacional conjunto, permanentemente ativado desde 2016, com capacidade interagências. Essa capacidade se destaca pela colaboração entre representantes de órgãos da Administração Pública Federal (APF), IC e outras entidades governamentais, instituições e empresas, tanto públicas quanto privadas, com relevância para a Defesa.

O SMDC é composto pelo órgão central, estruturas de DCiber das Forças Singulares, estruturas de GCiber dos Comandos Operacionais ativados e outras estruturas inseridas no sistema da administração central e ligadas ao MD. Embora os órgãos do SMDC nas Forças já existissem, sua criação oficial ocorreu apenas em 2020, indicando que o SMDC busca seu constante aperfeiçoamento. No âmbito político do SMDC, encontra-se o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), a quem compete planejar, coordenar e supervisionar as atividades de segurança da informação na APF, incluindo segurança cibernética, gestão de incidentes computacionais, proteção de dados, entre outros (Brasil, 2023d).

Para cumprir essa missão, o GSI/PR conta com a Secretaria de Segurança da Informação e Cibernética e seu respectivo Departamento de Segurança da Informação e Cibernética (DSI/GSI/PR), responsável, entre outras atribuições, por elaborar normativos e requisitos metodológicos, além de manter o Centro de

Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo (CTIR. Gov[14]). No contexto da APF, o CTIR Gov é o único *Computer Security Incident Response Team* (CSIRT) nacional, encarregado pela coordenação da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) (Brasil, 2022b).

As bases normativas para a segurança da informação na APF observam a Política Nacional de Segurança da Informação (PNSI), a Estratégia Nacional de Segurança Cibernética (E-Ciber) e o Plano de Gestão de Incidentes Cibernéticos (Plangic[15]). Além disso, estão relacionadas ao tema a Estratégia Brasileira para a Transformação Digital (E-Digital[16]) e a adesão à Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste[17].

O Exército Brasileiro (EB) desempenha um papel fundamental nas Forças Armadas Brasileiras, focando no desenvolvimento e na pesquisa na área de ciberdefesa e na proteção de instituições militares e governamentais. O Instituto Militar de Engenharia (IME) e o Centro de Defesa Cibernética (CDCIBER) são peças-chave na implementação dessas estratégias de defesa. O CDCIBER, subordinado ao MD nas Operações Conjuntas, possui um Estado-Maior conjunto responsável pelo planejamento e supervisão das ações, levando em conta as especificidades de cada Força Armada e promovendo a colaboração entre elas. É importante destacar seu papel crucial na segurança de grandes eventos, sendo um dos principais responsáveis por assegurar a PtçCiber durante essas ocasiões.

Em resumo, a Estrutura de Defesa Cibernética Nacional é um sistema complexo e coordenado que visa proteger os SD essenciais para a segurança e a estabilidade do país. Esta estrutura inclui uma rede integrada de órgãos governamentais, Forças Armadas, e agências especializadas, todos trabalhando em conjunto para monitorar, detectar e responder a ameaças cibernéticas.

---

14 Uma entidade responsável por receber, analisar e responder a notificações e eventos relativos a incidentes de segurança em sistemas computacionais (Brasil, 2023a).

15 Define os procedimentos para gerenciar incidentes cibernéticos entre os membros da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC) (Brasil, 2022b).

16 Apresenta um diagnóstico sobre os desafios a serem enfrentados para a transformação digital do País e propõe ações a serem implementadas com os objetivos de harmonizar as iniciativas do Poder Executivo Federal relacionadas ao ambiente digital (Brasil, 2022a).

17 Esta convenção trata sobre crimes cibernéticos e visa facilitar a cooperação internacional para o combate ao cibercrime (Brasil, 2023c).

3.2 ESTRUTURA DE DEFESA CIBERNÉTICA DA MB

Embora o EB desempenhe um papel central na pesquisa e na DCiber, é importante reconhecer que a MB também contribui significativamente para esses esforços. A MB está ativamente envolvida na proteção de suas próprias redes e sistemas contra ameaças cibernéticas, além de participar de iniciativas conjuntas de DCiber em nível nacional. Sua *expertise* e colaboração são essenciais para fortalecer as capacidades de DCiber do país como um todo.

A MB atua em três frentes na DCiber: capacitação de pessoal, por meio de cursos e palestras; estabelecimento e normatização de processos, visando a definição de procedimentos operacionais; implementação de tecnologias avançadas, incluindo redes seguras, *firewalls*[18] e *softwares* de proteção contra os ataques cibernéticos; e busca por vulnerabilidades nos SD em produção. Em sua doutrina de DCiber, a MB estabelece princípios, diretrizes e ações específicas, priorizando a capacitação contínua do pessoal. Como parte desses esforços, são realizadas simulações de DCiber, conhecidas como exercícios de GCiber, nos quais são exploradas as fragilidades dos SD, para fortalecer as competências da MB no enfrentamento de ameaças cibernéticas e capacitar seu pessoal em procedimentos de resposta a incidentes e de DCiber.

No contexto da Doutrina Cibernética da MB, o EMA atua no campo de DCiber, nível estratégico, estabelecendo a doutrina de DCiber, organizando e coordenando as atividades da MB e buscando a harmonização de esforços. O campo de GCiber, no nível de conflito cibernético, envolve as ações de PtçCiber, de Exploração Cibernética (ExpCiber) e de Ataque Cibernético (AtqCiber). Neste campo atuam o Comando de Operações Navais (ComOpNav), o Comando Naval de Operações Especiais (CoNavOpEsp), a DGMM, a DCTIM e o Centro de Tecnologia da Informação da Marinha (CTIM).

Compete ao ComOpNav emitir diretivas e regras de engajamento que orientem o treinamento e regulamentem o uso efetivo, tanto por suas unidades especializadas quanto em situações reais. Ao CoNavOpEsp cabe a formação de

---

18 “Solução de segurança baseada em *hardware* ou *software* (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas” (Alecrim, 2013, n.p).

Grupamentos Operativos de Guerra Cibernética (GptOpGCiber), capacitados para intervenções nos níveis operacional e tático, sempre que a ameaça cibernética demandar tal ação. À DCTIM compete a execução de atividades contínuas de prevenção e proteção imediata do ECiber de interesse da MB (ECiber-MBB[19]), respondendo prontamente a qualquer ameaça cibernética.

O CTIM desempenha um papel central na implementação das iniciativas de PtçCiber do ECiber-MB. Este Centro coordena diversas atividades, incluindo a operação da Central de Tratamento de Incidentes de Redes (CTIR), que é responsável pela integração com outras CTIRs das Forças Armadas e da estrutura governamental, como o CTIR.Gov e o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br[20]). Essas atividades envolvem a detecção, contenção, mitigação, correção e investigação de danos causados por atividades maliciosas no ambiente cibernético da MB (Brasil, 2021a), dentre as quais pode ser citada a identificação e a exploração de vulnerabilidades dos SD em produção na RECIM.

Por fim, recentemente foi criado o EsqdGCiber, oficialmente estabelecido pela Portaria nº 107/MB/MD/2024 (Brasil, 2024), subordinado ao CoNavOpEsp, com a missão de apoiar a execução das Ações de Guerra Cibernética (AGCiber[21]) na MB. O EsqdGCiber visa fortalecer as capacidades da MB em operações cibernéticas, garantindo que a instituição esteja devidamente preparada para enfrentar ameaças digitais que possam comprometer a segurança nacional (Brasil, 2020a). O EsqdGCiber desempenhará um papel crucial no suporte às iniciativas da MB e do ComDCiber, consolidando competências e recursos humanos, materiais, tecnológicos e financeiros voltados para a guerra cibernética. Esta criação representa um avanço estratégico significativo para a MB, aprimorando a capacidade dissuasória da Força Naval.

---

19 Uma parte do Espaço Cibernético que engloba os ativos de Tecnologia da Informação e Comunicações, nos quais a MB possui interesse operacional ou administrativo (Brasil, 2021a).

20 “Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional, gerido pelo NIC.br, uma entidade sem fins lucrativos vinculada ao Comitê Gestor da Internet no Brasil (CGI.br)” (Brasil, [s.d.], n.p).

21 Ações que utilizam ferramentas de Tecnologia da Informação e Comunicações para desestabilizar os ativos de informação do adversário (Brasil, 2017).

3.3 OPERAÇÕES CIBERNÉTICAS NA MB

A MB promove exercícios de GCiber como parte integrante de suas operações estratégicas. Esses exercícios são projetados para testar e aprimorar as capacidades da MB em lidar com ameaças cibernéticas, identificar vulnerabilidades existentes nos SD da MB, bem como para treinar seu pessoal em procedimentos de resposta a incidentes e DCiber. As operações de GCiber envolvem simulações de ataques cibernéticos, testes de vulnerabilidades em sistemas de informação e comunicação, e avaliação da prontidão e eficácia das medidas de segurança cibernética implementadas pela MB. Essas atividades são fundamentais para garantir a segurança e a integridade das operações navais em um ambiente digital cada vez mais complexo e desafiador. Dentre as operações cibernéticas da MB destacam-se: Octopus, Alligator, Ciber Securitas e Baluarte.

Durante a Operação ADEREX-Anfíbia/Superfície em maio de 2021, o Comando da Primeira Divisão da Esquadra (ComDiv-1) e o CoNavOpEsp realizaram o Exercício de Contraposição às Ameças Cibernéticas, conhecido como *Octopus*. Para tal, a 1ª Equipe de Exploração e Ataque da Divisão de Guerra, sob o comando do CoNavOpEsp, e um Destacamento de PtçCiber embarcaram no Navio-Aeródromo Multipropósito Atlântico, em busca de vulnerabilidades que pudessem comprometer os sistemas utilizados para Comando e Controle, além de realizar ações nos meios navais envolvidos na Operação (Brasil, 2021c). A operação contribuiu para treinar os militares dos navios envolvidos no emprego do sistema *Dreadnought* e na realização das AGCiber do tipo Exploração[22].

O sistema *Dreadnought* foi desenvolvido em 2017, pela Divisão de Guerra Cibernética (DivGCiber) do ComOpNav, cujo nome foi inspirado na classe de Encouraçados do início do século XX. Dentre suas funcionalidades, o sistema permite monitorar a rede, identificar, bloquear e reportar ameaças cibernéticas, além de construir uma consciência situacional a partir do monitoramento do ECiber. Em 2019, a DivGCiber passou a integrar o recém-ativado CoNavOpEsp e iniciou a condução das AGCiber. O CoNavOpEsp tornou-se o centro de desenvolvimento do

22 “Assume caráter furtivo na busca de dados e informações de interesse e no conhecimento de aspectos da estrutura do ECiber alvo, a fim de facilitar eventual AtqCiber ou obter vantagem na Dimensão Informacional” (Brasil, 2021a).

sistema *Dreadnought* e, atualmente, o sistema opera em mais de 20 OM, operativas e administrativas (Mota Junior; Martins, 2022).

A partir de 2020, o Sistema *Dreadnought* começou a ser empregado nos Exercícios de Contraposição às Ameaças Cibernéticas e, em 2021, expandiu suas operações para incluir não apenas meios navais, por meio do exercício denominado *Octopus*, mas também os Grupamentos Operativos de Fuzileiros Navais (GptOpFuzNav), com o exercício *Alligator*. Essas operações têm como objetivo principal aprimorar as capacidades de GCiber, tanto da Força Naval quanto dos GptOpFuzNav, ao mesmo tempo em que promovem uma mentalidade de PtçCiber dentro da MB. Dessa forma, o sistema *Dreadnought* se posiciona como um líder na PtçCiber operativa, ajudando a contrapor ameaças que possam explorar vulnerabilidades no ECiber de interesse da MB.

Em outubro de 2021, o CoNavOpEsp realizou a Operação Ciber Securitas VIII, que contou com a participação de seis Centros Locais de Tecnologia da Informação (CLTI): Comando em Chefe da Esquadra, Comando do 1º Distrito Naval (COM1ºDN), Comando da Força de Fuzileiros da Esquadra (ComFFE), Comando do 2º Distrito Naval (COM2º DN), Diretoria de Hidrografia e Navegação (DHN) e Comando do 7º Distrito Naval (COM7ºDN). As atividades da Operação Ciber Securitas VIII foram realizadas em um ambiente cibernético especialmente preparado e controlado pelo Laboratório de Ações Cibernéticas do CoNavOpEsp. Este ambiente é segregado da infraestrutura da Rede de Comunicações Integradas da Marinha (RECIM), garantindo um ambiente realista para as atividades, sem comprometer a Segurança da Informação. A operação proporcionou treinamento à Divisão de GCiber do CoNavOpEsp e aos membros dos CLTI, enfatizando as ações cibernéticas de Exploração e Proteção, respectivamente. Esse esforço contribuiu significativamente para fortalecer a mentalidade de DCiber na MB (Brasil, 2021).

Em agosto de 2020, o CoNavOpEsp liderou a Operação *Baluarte* XI, com a colaboração da DCTIM e do CTIM. A operação visou avaliar a resiliência dos SD e a eficácia dos procedimentos doutrinários da MB para realizar e mitigar ataques cibernéticos limitados, como os realizados por grupos hacktivistas. O exercício proporcionou uma oportunidade para fortalecer a cooperação entre os Setores

Operativo e do Material, além de contribuir para o desenvolvimento da capacidade de empreender ações cibernéticas ofensivas na MB (Brasil, 2020e).

3.4 LIMITAÇÕES DA DEFESA CIBERNÉTICA

As operações cibernéticas da MB têm como objetivo melhorar a execução das ações de GCiber para beneficiar as operações da Força Naval e dos GptOpFuzNav, e para auxiliar na disseminação da consciência e de práticas de PtçCiber dentro da MB, contribuindo com o aprimoramento da DCiber da MB. No entanto, a DCiber apresenta suas próprias limitações, destacando a importância e a necessidade de investimentos significativos nessa área estratégica, dadas as características distintas do ECiber.

Alguns aspectos do ECiber incluem a ausência de limitações geográficas, já que as ações de cibersegurança não se restringem a fronteiras físicas definidas; os agentes podem atuar de qualquer lugar e afetar qualquer região do mundo. Outro ponto é a fragilidade inerente, em que nenhum sistema é completamente seguro e todos estão expostos a possíveis ataques cibernéticos. Além disso, a abrangência global permite a execução de operações em escala mundial, simultaneamente em diversas frentes.

Dentre as principais limitações da segurança cibernética, podemos destacar diversos fatores críticos que impactam a eficácia das defesas e a proteção das informações. Em primeiro lugar, a complexidade das ameaças cibernéticas é um desafio constante. As ameaças estão se tornando cada vez mais sofisticadas e diversificadas, exigindo soluções de segurança avançadas e em constante evolução.

Outro problema significativo é a falta de recursos, pois as restrições financeiras e tecnológicas podem limitar os investimentos necessários para manter sistemas de segurança cibernética robustos e atualizados. A dependência de fornecedores também representa uma vulnerabilidade importante, visto que sistemas de terceiros, incluindo fornecedores e contratados, podem introduzir riscos à segurança cibernética, caso apresentem falhas ou vulnerabilidades.

Além disso, a capacitação e conscientização sobre segurança cibernética variam consideravelmente. Níveis inadequados de treinamento podem comprometer

a eficácia das medidas de defesa adotadas pela organização. A coordenação e integração das estratégias de segurança cibernética dentro da organização também pode ser um desafio operacional. Integrar e coordenar eficazmente as diversas abordagens de segurança requer um esforço significativo. A regulamentação e a conformidade representam outra limitação importante, pois cumprir com normas e regulamentos de segurança cibernética pode ser complexo e exige recursos adicionais para garantir que todas as exigências sejam atendidas.

A velocidade na resposta a incidentes cibernéticos é outro fator crítico. A capacidade de identificar, mitigar e responder rapidamente a incidentes pode ser limitada pela complexidade dos sistemas e das ameaças. Por fim, manter sistemas de informação e comunicação seguros em um ambiente operacional complexo e em constante mudança é um desafio técnico que demanda inovação e adaptação constante.

Além disso, dentre as limitações de DCiber citadas na Doutrina de Guerra Cibernética da MB (Brasil, 2021a) destacam-se a presença de vulnerabilidades nos sistemas de informação e o risco de surpresas devido às vulnerabilidades dos próprios sistemas de informação. Essas limitações sublinham a necessidade contínua de investimentos, treinamentos e colaboração para fortalecer a DCiber da MB contra ameaças emergentes e persistentes. Portanto, é crucial buscar soluções para aprimorar a segurança dos SD da MB com o objetivo de mitigar ou minimizar a possibilidade de sucessos dos ataques cibernéticos.

No próximo capítulo, serão discutidas as falhas dos processos de desenvolvimento e de homologação dos SD da MB. Além do mais, será apresentada uma proposta para aprimorar os processos de homologação de SD e de hospedagem de SD no CD-MB, com o objetivo de melhorar a segurança dos SD e, consequentemente, aumentar a PtçCiber da RECIM contra as ameaças cibernéticas.

4 DESENVOLVIMENTO E HOMOLOGAÇÃO DE SISTEMAS DIGITAIS NA MB

É crescente a necessidade das OM de desenvolver ou obter sistemas para automatizar diversos processos que atualmente são executados de forma manual. Para tanto, as OM que possuem equipe de desenvolvimento, desenvolvem os seus

sistemas internamente, enquanto que aquelas que não possuem, optam por contratar o desenvolvimento por empresa terceirizada ou pelo Centro de Análise de Sistemas Navais (CASNAV). Este último é uma OM Prestadora de Serviços (OMPS), reconhecida como referência no desenvolvimento de sistemas na MB. Além disso, também ocorre a aquisição de sistemas de prateleira do tipo *Comercial Off-the-shelf System* (COTS) ou do tipo *Modified* COTS (MOTS), que podem ser customizados para atender as necessidades específicas de uma organização.

De acordo com as Normas de Tecnologia da Informação da Marinha – DGMM-0540 (Brasil, 2019a), um SD possui cinco fases de ciclo de vida, que compreende o Planejamento, a Obtenção, a Produção, a Manutenção e a Desativação. Durante a fase de planejamento é previsto o processo de conformidade do sistema, que consiste na verificação da conformidade da solução com as normas em vigor, como a DCTIMBOTEC 30/002/2023, que trata da padronização de tecnologias de desenvolvimento na MB e a DCTIMARINST 30-17, que trata da adequação dos SD e Banco de Dados da MB às boas práticas de segurança para proteção dos Dados Pessoais. Além do mais, é verificado se a solução proposta pode impactar o funcionamento da RECIM e se há um SD disponível na MB que atenda a demanda apresentada, para evitar redundância de sistemas. A partir do parecer favorável da OM responsável pelo negócio que está sendo automatizado, chamada de OM Regulamentadora (OMREL) e da conformidade da solução com as normas em vigor, a DCTIM autoriza o desenvolvimento ou a aquisição do SD (Brasil, 2019b).

A fase de obtenção tem o objetivo de avaliar a necessidade de desenvolvimento de um novo SD ou a manutenção de um SD em produção. A fase de produção caracteriza-se pela disponibilidade do SD na RECIM após o cumprimento das etapas do processo de homologação da DCTIM. A fase de manutenção de *software* é importante para garantir que o SD continue a ser eficaz, seguro e útil ao longo de seu ciclo de vida operacional. A desativação compreende a última fase do ciclo de vida de um SD, quando o *software* não atende mais às necessidades da organização ou quando é substituído por uma nova versão ou tecnologia.

No processo de homologação de SD, a OMSOL precisa enviar alguns documentos do sistema para a DCTIM, previstos na DCTIMARINST 33-06B, que trata da conformidade, homologação e hospedagem de SD. Após a verificação da documentação, a DCTIM emite o Parecer de Análise Básica das Características de SID para Homologação de SD, com as discrepâncias de segurança encontradas na documentação. Adicionalmente, o CTIM realiza as varreduras de segurança no SD, que consistem na avaliação do código-fonte e da infraestrutura do servidor do SD, em busca de vulnerabilidades de segurança. O CTIM elabora o Relatório de Análise de Vulnerabilidades que apresenta as vulnerabilidades encontradas e envia para o responsável pelo SD. Após a correção das discrepâncias e das vulnerabilidades de segurança, a DCTIM classifica o SD como homologado. Caso o SD utilize tecnologias obsoletas ou não atenda algum dos requisitos previstos na norma, a DCTIM classifica o SD como legado ou não homologado, respectivamente (Brasil, 2019b).

Para obtenção das informações sobre os processos de desenvolvimento e de homologação de SD na MB, e a incidência de ataques cibernéticos aos SD da MB, a metodologia utilizada foi a realização de duas entrevistas, uma com o atual Chefe do Departamento de Sistemas Digitais da DCTIM e outra com o atual Encarregado do CTIR do CTIM, responsáveis pela homologação de SD e pelo monitoramento de incidentes cibernéticos na MB, respectivamente.

Essas entrevistas foram fundamentais para descobrir quais tarefas dos processos de desenvolvimento e homologação de sistemas poderiam ser aprimoradas. Dessa forma, de acordo com o Apêndice A, no âmbito da defesa cibernética, uma das preocupações da DCTIM e do CTIM reside nos sistemas hospedados na DMZ. Apesar de serem homologados, os administradores desses sistemas mantêm acesso ao ambiente de produção, o que possibilita modificações no código-fonte e a instalação de novas aplicações no servidor. Essas ações podem acarretar novas vulnerabilidades de segurança e abrir portas lógicas, facilitando o acesso indevido ao banco de dados do próprio sistema e de outros sistemas, além de comprometer a segurança da RECIM, ao permitir acesso aos sistemas da rede interna da MB por possíveis atacantes.

O desenvolvimento de SD na MB é descentralizado, com várias OM responsáveis por essa tarefa, embora a Doutrina de Tecnologia da Marinha – EMA-416 defina que os Órgãos de desenvolvimento de Sistemas de TI são: Centro Tecnológico da Marinha em São Paulo (CTMSP), Centro de Análises de Sistemas Navais (CASNAV), Instituto de Estudos do Mar Almirante Paulo Moreira (IEAPM) e Instituto de Pesquisas da Marinha (IPqM). Como resultado, a MB possui mais de 450 SD hospedados na RECIM sob a responsabilidade de 95 OM, muitos dos quais apresentam funcionalidades redundantes, como o cadastro de usuários e de OM. O catálogo desses sistemas encontra-se disponível em site intranet da MB e muitos desses sistemas são legados, pois utilizam tecnologias obsoletas as quais aumentam as vulnerabilidades da RECIM.

Cerca de 110 SD estão atualmente hospedados no CD-MB, localizado fisicamente no CTIM, onde são monitorados continuamente, conforme descrito no Apêndice A. Antes de serem hospedados, todos os SD passam pelo processo de homologação, no entanto nem todos os SD hospedados na rede interna da OM foram submetidos a esse processo, o que significa que a DCTIM não tem conhecimento da existência desses sistemas.

Para os sistemas que precisam ser acessados pela internet, é necessário que estejam hospedados na DMZ do CD-MB. Isso implica que esses SD devem obrigatoriamente ser submetidos ao processo de homologação, no qual todas as vulnerabilidades de segurança identificadas precisam ser corrigidas antes do sistema ser colocado em produção.

Em virtude da diversidade de OM que desenvolvem sistemas, a grande maioria não adota metodologias e melhores práticas de desenvolvimento seguro, por não terem uma equipe de desenvolvimento dedicada, possuindo somente um desenvolvedor responsável por todas as etapas, desde a análise dos requisitos e codificação até os testes e manutenção do sistema. Além disso, esse desenvolvedor pode nem mesmo ser da área de TI. Isso resulta na ausência de testes de segurança durante o processo de desenvolvimento.

Esses tipos de teste podem ser divididos em dinâmicos, *Dynamic Application Security Testing (*DAST) e estáticos, *Static Application Security Testing* (SAST). Enquanto o DAST permite analisar uma aplicação *web* em execução para encontrar

vulnerabilidades, o SAST permite acessar o código-fonte da aplicação *web* para identificar falhas de *software* e vulnerabilidades críticas.

Durante o processo de homologação do SD, o CTIM realiza varredura nas aplicações *web* utilizando exclusivamente ferramentas do tipo DAST, devido à falta de acesso ao código-fonte dos sistemas, uma vez que a OM responsável pelo SD não o disponibiliza para o CTIM. Como resultado, os SD podem ser colocados em produção sem que todas as vulnerabilidades de código sejam identificadas durante essas varreduras. Essa limitação ocorre porque o CTIM não emprega ferramentas SAST, devido à indisponibilidade do código-fonte fornecido pela OM responsável pelo SD.

De acordo com a entrevista do Apêndice A, no período de abril a junho de 2024, as ferramentas de segurança do CTIM bloquearam 2.012.148 ataques provenientes da Internet, com destino à RECIM. Das tentativas de ataque, 1.962.522 eventos foram direcionados aos SD, o que representa cerca de 97% do total. Portanto, esses dados indicam que os sistemas da MB são alvos significativos para os atacantes, reforçando a preocupação com a segurança cibernética e a importância crítica da proteção desses SD.

4.1 METODOLOGIA DE DESENVOLVIMENTO, SEGURANÇA E OPERAÇÕES (DEVSECOPS)

Existem diversos modelos de ciclo de vida de SD, como cascata, espiral, ágil e desenvolvimento e operações (DevOps). Poucos desses modelos abordam detalhadamente a segurança de *software*, sendo necessário incorporar práticas de segurança no desenvolvimento de sistemas em cada modelo, de forma integrada.

Independentemente do modelo de ciclo de vida utilizado, é importante integrar práticas seguras de desenvolvimento de *software* para minimizar a quantidade de vulnerabilidades e reduzir o impacto potencial de falhas não detectadas. Embora a segurança possa ser abordada em diversas fases do ciclo de vida, em geral, quanto mais cedo a segurança for incorporada no desenvolvimento do sistema, menor será o esforço e o custo necessários para atingir o mesmo nível de proteção (Dodson; Souppaya; Scarfone, 2020).

Portanto, visando melhorar a segurança dos SD da MB e consequentemente fortalecer a segurança da RECIM contra ataques cibernéticos, propõe-se a adoção da metodologia DevSecOps no desenvolvimento de sistemas. Esta abordagem combina práticas de desenvolvimento de *software* (Dev), segurança (Sec) e operações (Ops), em um processo contínuo de entrega de *software*. O DevSecOps integra a segurança desde as fases iniciais do desenvolvimento, junto com práticas de aprimoramento contínuo. Adicionalmente, ferramentas e processos automatizados garantem que o *software* seja avaliado e testado a cada modificação no código-fonte, eliminando potenciais vulnerabilidades e falhas de segurança.

A metodologia DevSecOps oferece uma série de benefícios significativos para a área de desenvolvimento, como: entrega ágil de software, facilitada pela integração entre as equipes de desenvolvimento, segurança e operações; diminuição de incidentes, graças à detecção precoce de vulnerabilidades e à implementação de medidas preventivas; redução de custos, uma vez que a identificação precoce de vulnerabilidades de segurança previne retrabalho e perdas financeiras; e aprimoramento contínuo da segurança, ao educar as equipes sobre práticas de segurança desde o início do desenvolvimento, com foco em agregar valor à proteção e diminuir a frequência de invasões. Essa abordagem não apenas melhora a eficiência operacional, mas também fortalece a resiliência dos sistemas contra ameaças cibernéticas.

Cabe ressaltar que a metodologia DevSecOps é amplamente adotada por muitas empresas devido à sua capacidade de integrar segurança em todas as fases do ciclo de desenvolvimento, proporcionando uma abordagem mais eficiente e proativa para gerenciar riscos de segurança. No entanto, a sua adoção tende a ser mais lenta em organizações como a MB por vários motivos. Primeiramente, as instituições públicas frequentemente lidam com sistemas legados complexos que podem não estar alinhados com as práticas modernas de DevSecOps. Isso torna a transição para novas metodologias mais desafiadora, dado que adaptar sistemas existentes pode exigir significativas mudanças estruturais e técnicas.

Além disso, a cultura e os processos nas forças armadas são mais rígidos e tradicionais, o que pode retardar a adoção de novas metodologias e tecnologias. A implementação de DevSecOps pode necessitar de mudanças culturais e

operacionais profundas que nem sempre são fáceis de realizar em instituições com práticas estabelecidas há muito tempo. Considerações específicas de segurança e confidencialidade também desempenham um papel importante. As forças armadas frequentemente lidam com requisitos de segurança e confidencialidade que exigem abordagens especializadas e mais cautelosas, o que pode impactar a implementação de práticas padrão de DevSecOps.

Por fim, as prioridades e o orçamento das OM se concentram em diferentes aspectos de segurança e tecnologia. Isso pode limitar a alocação de recursos para a adoção de novas metodologias, especialmente quando outras demandas são mais urgentes ou prioritárias. Cada organização tem suas próprias prioridades e desafios, e a transição para metodologias modernas como DevSecOps pode levar tempo, especialmente em instituições com estruturas e necessidades muito específicas como a MB.

4.2 SOLUÇÃO PROPOSTA

Independente das tecnologias a serem utilizadas nos futuros SD da MB, o novo processo de desenvolvimento e homologação de sistemas será capaz de prover a segurança necessária aos SD em todo o seu ciclo de vida, permitindo a migração gradual dos sistemas legados e a mudança da atual metodologia para a nova, que está sendo proposta neste estudo.

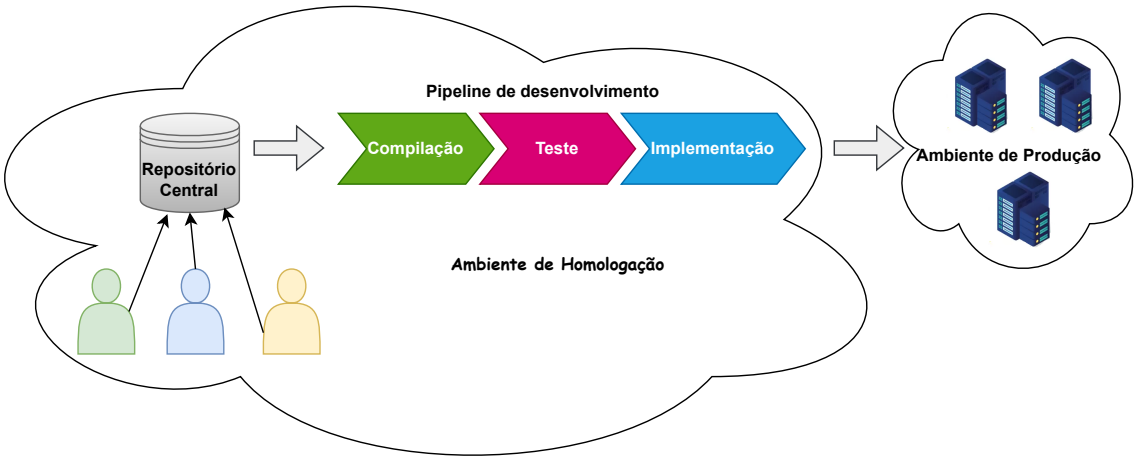
Antes de implementar a solução, será necessário conduzir uma pesquisa com as OM responsáveis pelo desenvolvimento de SD na MB e que possuem uma equipe de desenvolvimento dedicada, conforme roteiro de pesquisa descrito no Apêndice B deste trabalho. O resultado dessa pesquisa auxiliará na escolha das tecnologias de desenvolvimento que serão agregadas ao novo processo de desenvolvimento e homologação de SD, e também, a identificar quais etapas da metodologia DevSecOps poderão ser utilizadas no primeiro momento, de acordo com a experiência dos desenvolvedores das OM.

A Figura 1 ilustra as etapas do novo processo de desenvolvimento e homologação de sistemas na MB, que deve ser executado de forma progressiva, acompanhando a evolução do processo. Inicialmente, a DCTIM precisa estabelecer

um repositório centralizado de código-fonte no CD-MB, permitindo que os desenvolvedores armazenem e gerenciem as versões dos sistemas desenvolvidos. Esse repositório facilitará a colaboração entre os desenvolvedores da OM, promovendo o compartilhamento e o reúso eficiente do código-fonte.

À medida que as OM se familiarizarem com o uso desse repositório, a próxima etapa consistirá na implementação de um *pipeline* de desenvolvimento. Esse *pipeline* é composto por um conjunto de etapas automatizadas e interconectadas que permitem a entrega contínua e eficiente de *software*. Essas etapas são organizadas sequencialmente de forma a guiar o código-fonte desde a fase inicial de desenvolvimento até a sua implantação e eventual manutenção. O *pipeline* de desenvolvimento deverá incluir as etapas de compilação, teste e implementação, conhecidas em inglês como *build*, *test* e *deploy*, respectivamente.

Figura 1 – Etapas do novo processo de desenvolvimento e homologação de sistemas na MB



Fonte: O Autor

A etapa de compilação se inicia quando os desenvolvedores alteram o código-fonte e enviam as alterações para o repositório central, conhecidas em inglês como *commit.* Nessa etapa são realizadas a análise automatizada de segurança, a análise de componentes de *software*, o teste de *software* de aplicação estática (SAST) e testes de unidade. Cabe ressaltar a importância da análise das dependências de código externo, uma vez que estas podem conter vulnerabilidades tanto intencionais quanto não e que podem comprometer o sistema.

Após o código-fonte ter sido compilado com sucesso, a etapa de teste é acionada. Nesta fase são utilizadas ferramentas de teste dinâmico de segurança de aplicações (DAST), para identificar, em tempo real, os fluxos de aplicativos, como autenticação de usuário, autorização, injeção de SQL e endpoints[23] de API. O teste DAST, focado em segurança, analisa o aplicativo em relação a uma lista de problemas graves conhecidos, como os destacados no OWASP Top 10.

Se as fases anteriores forem aprovadas, o código-fonte será implantado no ambiente de produção e o SD começará a ser monitorado pelo CTIM. Dessa forma, o processo de homologação será integrado às etapas do processo de desenvolvimento, com o sistema sendo homologado somente após a aprovação bem-sucedida de todas as etapas do *pipeline* de desenvolvimento. A documentação do sistema deverá ser armazenada no repositório centralizado, permitindo que a DCTIM tenha acesso tanto ao código-fonte quanto à documentação associada ao sistema.

À medida que o desenvolvedor modificar o código-fonte do sistema, a alteração será submetida a uma análise de vulnerabilidades antes de ser implantada no servidor de produção que hospeda o SD. No entanto, um código-fonte que está seguro hoje pode não permanecer seguro amanhã, em virtude do surgimento de novas vulnerabilidades, sendo assim, é fundamental que o CTIM realize varreduras de vulnerabilidades periódicas com ferramentas DAST nos SD da DMZ. Isso permitirá identificar novas falhas de segurança as quais deverão ser reportadas à OM responsável pela manutenção do sistema, para correção das respectivas vulnerabilidades.

23 Pontos de acesso específicos em uma interface de programação de aplicativos (API) que permitem que sistemas externos se comuniquem com o serviço ou aplicativo que disponibiliza a API.

O objetivo da citada metodologia é aplicar esse novo processo de desenvolvimento e homologação de SD aos novos projetos de desenvolvimento de sistemas e, à medida que o processo evoluir, as OM deverão planejar a modernização dos sistemas legados para adotar essa metodologia. Para a implantação desse novo processo, será necessária a aquisição de ferramentas que apoiem as etapas do processo, como *GitLab* e *SonarQube* e, por isso, é crucial destacar a necessidade de capacitação dos desenvolvedores das OM na metodologia DevSecOps e no uso das ferramentas envolvidas nesse processo.

Cabe ressaltar que o ComDCiber oferece anualmente o curso de guerra cibernética para oficiais e praças, com a disponibilização de algumas vagas para a MB. Após a conclusão do curso, os participantes são designados para atuar na DCTIM, no CoNavOpEsp ou no CTIM, com a missão de implementar as melhores práticas de segurança para a PtçCiber da RECIM. Diante disso, seria altamente recomendável incluir, nos cursos de formação de oficiais e praças da área de TI, uma disciplina dedicada à segurança da informação e à segurança no desenvolvimento de SD.

Ao final desta seção, conclui-se que o modelo apresentado na Figura 1 apresenta uma proposta para iniciar o desenvolvimento de SD seguros na MB. O objetivo desse modelo é melhorar a PtçCiber da RECIM, uma vez que o número de tentativas de ataque aos SD da RECIM é significativamente elevado, conforme detalhado na entrevista do Apêndice A.

5 CONSIDERAÇÕES FINAIS

Este estudo identificou um possível aprimoramento dos processos de desenvolvimento e homologação de SD para melhorar a segurança dos SD da MB. Foi necessário fazer a apresentação dos principais conceitos relacionados com o tema. Inicialmente, foi apresentado um histórico de ataques cibernéticos, além dos principais tipos de ataques e vulnerabilidades cibernéticas.

Na sequência, discutiu-se a importância da DCiber como componente essencial da END, destacando o papel central do EB na pesquisa nessa área e a contribuição significativa da MB para esse campo. Constatou-se que a MB tem

aprimorado a sua capacidade de DCiber por meio da realização de operações cibernéticas que simulam ataques cibernéticos reais e que essas ações contribuem para a identificação de falhas de segurança da informação nos SD hospedados na RECIM.

Além disso, a MB está aprimorando a sua capacidade de DCiber com o investimento em novas tecnologias de segurança e com a criação de organizações dedicadas à PtçCiber, como o Esquadrão de Guerra Cibernética. No entanto, uma das principais limitações da DCiber é a vulnerabilidade nos sistemas de informação, sendo necessário que a MB aprimore a sua capacidade de identificação e correção de vulnerabilidades dos seus SD, prevenindo potenciais comprometimentos da RECIM frente a ataques cibernéticos.

Em seguida, foi necessário compreender o contexto atual da MB em relação à estrutura de defesa e PtçCiber, às operações de GCiber e aos processos de desenvolvimento e homologação de SD. O cenário identificado foi analisado e detalhado por meio de entrevistas, análise das normas relacionadas e compreensão dos processos de desenvolvimento e homologação dos SD. Esse entendimento permitiu identificar fragilidades e limitações, possibilitando a proposição de uma solução destinada a eliminar essas deficiências e fortalecer a segurança.

Conclui-se, portanto, que este estudo demonstrou como a DCTIM, com o apoio das OMs desenvolvedoras, pode aprimorar os processos de desenvolvimento e homologação de SD e contribuir para o aperfeiçoamento da PtçCiber da RECIM. O objetivo é integrar a segurança ao longo do desenvolvimento e, por consequência, a homologação do SD se dará de forma automatizada, com base na aprovação dos sistemas nas etapas do *pipeline* de desenvolvimento. Com essas melhorias, a MB será capaz de desenvolver sistemas mais seguros e proteger a RECIM contra ataques cibernéticos.

Adicionalmente, a contínua adaptação às novas ameaças e a evolução tecnológica são cruciais para manter a eficácia da DCIber, garantindo que a MB não apenas responda adequadamente às ameaças emergentes, mas também se antecipe a elas, consolidando uma postura defensiva, robusta e dinâmica.

REFERÊNCIAS

ALECRIM, E. **O que é um firewall? Definição e explicação**. Disponível em: https://www.infowester.com/firewall.php. Acesso em: 07 nov. 2024.

ASLAN, Ö. *et al*. **A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions**. Electronics (2079-9292), v. 12, n. 6, 2023.

BRASIL. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)**. Disponível em: https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/sisp/guia-do-gestor/seguranca_e_privacidade/orgao-que-atuam-com-privacidade-e-seguranca/centro-de-estudos-resposta-e-tratamento-de-incidentes-de-seguranca-no-brasil-cert-br. Acesso em: 10 jun. 2024.

BRASIL, G. DE S. I. DA P. DA R. **CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo**. 2023, 2023a.

BRASIL, M. **Doutrina Militar Naval (EMA-305)**. Brasilia, DF, 2017.

BRASIL, M. **Normas de Tecnologia da Informação da Marinha (DGMM-540)**. 3. ed. Rio de Janeiro, RJ. 2019, 2019a.

BRASIL, M. **Norma sobre Conformidade, Homologação e Hospedagem de Sistemas Digitais (SD) na MB (DCTIMARINST 33-06B)**. Rio de Janeiro, RJ, 2019. 2019b.

BRASIL, M. **Plano Estratégico da Marinha (PEM 2040)**. Brasilia, DF: 2020, 2020a.

BRASIL, M. **Comando Naval de Operações Especiais conduz exercício de Guerra Cibernética | Marinha do Brasil**. 2020. Disponível em: https://www.marinha.mil.br/noticias/comando-naval-de-operacoes-especiais-conduz-exercicio-de-guerra-cibernetica. Acesso em: 15 jun. 2024b.

BRASIL, M. **Doutrina Cibernética da Marinha (EMA-419)**. 1ª ed. Brasília, DF: 2021, 2021a.

BRASIL, M. B., com informações da Marinha do. **CoNavOpEsp realiza Operação "Ciber Securitas VIII"**. 2021. Disponível em: https://www.defesaemfoco.com.br/conavopesp-realiza-operacao-ciber-securitas-viii/. Acesso em: 15 jun. 2024b.

BRASIL, M. DA C., Tecnologia e Inovações. Portaria MCTI nº 6.543, de 16.11.2022. **Aprova a Estratégia Brasileira para a Transformação Digital (E-Digital) para o ciclo 2022-2026**. 2022, 2022a.

BRASIL, M. DA D. **Estratégia Nacional de Defesa. Política Nacional de Defesa.** 2020, 2020c. Disponível em:

https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/pnd_end_congresso_.pdf. Acesso em: 2 jun. 2024.

BRASIL, M. DA D. PORTARIA Nº 3.781/GM-MD, DE 17 DE NOVEMBRO DE 2020. **Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências**. 2020, 2020d.

BRASIL, M. DA D. Portaria GM-MD n° 5.081, de 16 de outubro de 2023 **Aprova a Doutrina Militar de Defesa Cibernética** - MD31-M-07. n. 2ª, p. 46, 2023, 2023b.

BRASIL, M. DA D. PORTARIA N. 107/MB/MD, DE 29 DE MAIO DE 2024. **Cria o Esquadrão de Guerra Cibernética e dá outras providências**. 2024.

BRASIL, M. DO B. Portaria normativa n° 3.389/MD, de 21 de dezembro de 2012. **Dispõe sobre a Política Cibernética de Defesa**: MD31-P-02. n. 1ª, p. 24, 2012.

BRASIL, M. DO B. **Navios da Esquadra realizam exercício de Guerra Cibernética durante a Operação "ADEREX-Anfíbia/Superfície 2021"**. 2021. Disponível em: https://www.marinha.mil.br/noticias/navios-da-esquadra-realizam-exercicio-de-guerra-cibernetica-durante-operacao-aderex. Acesso em: 15 jun. 2024c.

BRASIL, P. DA R. PORTARIA GSI/PR Nº 120, DE 21 DE DEZEMBRO DE 2022. **Aprova o Plano de Gestão de Incidentes Cibernéticos para a administração pública federal**. 2022, 2022b.

BRASIL, P. DA R. DECRETO Nº 11.491, DE 12 DE ABRIL DE 2023. **Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001**. 2023, 2023c.

BRASIL, P. DA R. DECRETO Nº 11.676, DE 30 DE AGOSTO DE 2023. **Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão, das Funções de Confiança e das Gratificações do Gabinete de Segurança Institucional da Presidência da República**. 2023 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11676.htm#art5. Acesso em: 8 jun. 2024.

BUKHARI, S. N.; DAR, M. A.; IQBAL, U. **Reducing attack surface corresponding to Type 1 cross-site scripting attacks using secure development life cycle practices**. 2018 4th International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-informatics (AEEICB). IEEE, 2018. Disponível em: https://ieeexplore.ieee.org/abstract/document/8480945/. Acesso em: 4 mai. 2024.

CORREIA, F.; RIGUES, R. **Falha crítica no Windows permite ação remota de invasores - Olhar Digital**. 2021. Disponível em: https://olhardigital.com.br/2021/07/02/reviews/falha-critica-no-windows-permite-acao-remota-de-invasores/. Acesso em: 8 set. 2024.

OLIVEIRA, D. **Firmware: o que é e por que você deve atualizá-lo - Olhar Digital**. Disponível em: https://olhardigital.com.br/2023/09/28/dicas-e-tutoriais/firmware-o-que-e-e-por-que-voce-deve-atualiza-lo/. Acesso em: 17 ago. 2024.

DENNING, D. E. **Stuxnet: What Has Changed?** Future Internet, v. 4, n. 3, p. 672–687, 2012.

DODSON, D.; SOUPPAYA, M.; SCARFONE, K. **Mitigating the risk of software vulnerabilities by adopting a secure software development framework (ssdf)**. NIST: Gaithersburg, MD, USA, 2020.

FEBRABAN. **Brasil é segundo país mais atingido por ciberataques na América Latina, diz relatório**. 2023. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-e-segundo-pais-mais-atingido-por-ciberataques-na-america-latina-diz-relatorio. Acesso em: 3 ago. 2024.

FORTINET. **O que é uma DMZ e por que você a usaria?** Disponível em: https://www.fortinet.com/br/resources/cyberglossary/what-is-dmz.html. Acesso em: 1 jul. 2024.

GOUTAM, A.; TIWARI, V. **Vulnerability assessment and penetration testing to enhance the security of web application**. 2019 4th International Conference on Information Systems and Computer Networks (ISCON). IEEE, 2019. Disponível em: https://ieeexplore.ieee.org/abstract/document/9036175/. Acesso em: 4 mai. 2024.

MARTIN, D. M. **Tracing the Lineage of DarkSeoul**. 2015, 2015a. Disponível em: https://sansorg.egnyte.com/dl/nurZpNn8ee. Acesso em: 4 set. 2024.

MOTA JUNIOR, S. M.; MARTINS, N. L. **Sistema Dreadnought**: **Revista Passadiço**, v. 34, n. 42, p. 50–50, 2022.

OLIVEIRA, D. **Firmware: o que é e por que você deve atualizá-lo - Olhar Digital**. 2023. Disponível em: https://olhardigital.com.br/2023/09/28/dicas-e-tutoriais/firmware-o-que-e-e-por-que-voce-deve-atualiza-lo/. Acesso em: 17 ago. 2024.

OWASP. **Sobre OWASP - OWASP Top 10:2021**. Disponível em: https://owasp.org/Top10/pt_BR/A00-about-owasp/. Acesso em: 18 mai. 2024.

PATEL, K. **A survey on vulnerability assessment & penetration testing for secure communication**. 2019. 3rd International Conference on Trends in Electronics and Informatics (ICOEI). IEEE, 2019. Disponível em: https://ieeexplore.ieee.org/abstract/document/8862767/. Acesso em: 4 mai. 2024.

SANTANA, B. **O Que é HTTP e Como Ele Permite o Acesso ao Seu Site**. **Hostinger Tutoriais**, 2023. Disponível em: https://www.hostinger.com.br/tutoriais/http. Acesso em: 8 set. 2024.

SIDDIQUI, MOHD. S.; VERMA, D. **Cross site request forgery: A common web application weakness**. 2011. IEEE 3rd International Conference on Communication Software and Networks. Disponível em: https://ieeexplore.ieee.org/abstract/document/6014783. Acesso em: 18 mai. 2024.

WEAMIE, S. J. Y. **Cross-Site Scripting Attacks and Defensive Techniques: A Comprehensive Survey**. International Journal of Communications, Network and System Sciences, v. 15, n. 8, p. 126–148, 2022.

WORLD ECONOMIC FORUM. **The Global Risks Report 2024**. n. 19, 2024. Relatório. Disponível em: https://www.weforum.org/publications/global-risks-report-2024. Acesso em: 20 mai. 2024.

ZACKS, A. **Análise do AhnLab Antivirus em 2024 — Será que ele é bom?** 2024. Disponível em: https://pt.safetydetectives.com/best-antivirus/ahnlab/. Acesso em: 8 set. 2024.

APÊNDICE A — Entrevistas

Data: 24 de julho de 2024

Entrevistado..: Capitão de Fragata José WALDOMIRO Sinico Júnior

Função.....: Chefe do Departamento de Sistemas Digitais da DCTIM

1 – Qual é a principal preocupação da DCTIM em relação aos Sistemas Digitais?

Resp.: O processo de homologação já prevê a análise de vulnerabilidades de segurança dos sistemas, no entanto, os administradores desses sistemas continuam com acesso ao ambiente de produção, possibilitando novas modificações no código-fonte e permitindo que novas vulnerabilidades de segurança sejam introduzidas no sistema.

2 – Quantos sistemas digitais aproximadamente estão hospedados no CD-MB?

Resp.: Estão hospedados no CD-MB aproximadamente 110 sistemas.

3 – Quais problemas do processo de desenvolvimento que refletem na segurança dos SD?

Resp.: O desenvolvimento de sistemas digitais na MB é descentralizado, o que resulta na criação de sistemas com funcionalidades redundantes. Além disso, a maioria das equipes de desenvolvimento das OM não segue metodologias de desenvolvimento seguro, o que leva à criação de sistemas com vulnerabilidades de segurança.

Data: 23 de julho de 2024

Entrevistado..: Capitão de Corveta (EN) DANILO Fernandes de Assis

Função.....: Encarregado do Centro de Tratamento de Incidentes do CTIM

1 – Quantos ataques, provenientes da Internet com destino à Rede de Comunicações Integrada da Marinha (RECIM), foram bloqueados nos últimos 3 meses pelas ferramentas de segurança utilizadas pelo CTIM?

Resp.: 2.012.148 eventos de bloqueio.

2 – Destas tentativas de ataque, quantas tiveram como alvo os Sistemas Digitais da MB?

Resp.: 1.962.522 eventos direcionados aos Sistemas Digitais (MB) (~ 97%).

3 – O CTIM realiza algum monitoramento de segurança nos Sistemas Digitais que estão hospedados no Centro de Dados da Marinha do Brasil (CD-MB)?

Resp.: Sim, há um monitoramento contínuo dos ativos e serviços hospedados no Centro de Dados da Marinha do Brasil (CD-MB), principalmente os mais críticos.

APÊNDICE B — Roteiro de Pesquisa de Avaliação de Desenvolvimento de Sistemas Digitais

1 – A OM possui quantos sistemas sob sua responsabilidade?

R: _____

2 – A OM possui sistemas legados, que utilizam tecnologias obsoletas?

(a) sim

(b) não

3 – Os SD da OM foram submetidos ao processo de homologação da DCTIM?

(a) sim, todos os sistemas são homologados

(b) sim, mas nem todos os SD foram submetidos ao processo de homologação

(c) não, todos os sistemas não são homologados

4 – Qual o tipo de metodologia de desenvolvimento é utilizada?

(a) Cascata

(b) Espiral

(c) Ágil

(d) DevOps

(e) DevSecOps

5 – A equipe de desenvolvimento é composta por quantas profissionais?

(a) de 1 a 2 pessoas

(b) de 3 a 5 pessoas

(c) de 6 a 9 pessoas

(d) mais que 10 pessoas

6 – A OM utiliza *pipeline* de desenvolvimento?

(a) sim

(b) não

7 – Se a alternativa anterior foi verdadeira, qual a ferramenta de *pipeline* é utilizada para automatizar o desenvolvimento?

R: _____

8 – Durante o desenvolvimento dos sistemas, são realizados testes de segurança de código?

(a) sim

(b) não

9 – Se a alternativa anterior foi verdadeira, qual a ferramenta de segurança é utilizada para analisar o código-fonte?

R: _____

10 – A OM utiliza *containers* no desenvolvimento dos SD?

(a) sim

(b) não

11 – Se a alternativa anterior foi verdadeira, qual a ferramenta de *container* é utilizada?

R: _____