UTILIZAÇÃO DE RASPBERRY COMO GATEWAY DE ANONIMIZAÇÃO

S Ten Marcio **Da Silveira** Pinto
Sgt Lucas Pimentel **Diniz**

RESUMO

Neste século XXI viu-se uma expansão dos meios de tecnologia da informação. Tamanho foi este crescimento, que por muitas vezes o mundo digital se confunde com o real. As pessoas adotam um estilo de vida digital para várias rotinas e ações em seu dia a dia. Um exemplo está em como lidamos com nossas operações financeiras. Qualquer que seja a necessidade, não há mais a obrigatoriedade de irmos a uma agência fisíca. Uma vasta gama de situações são resolvidas através de um aplicativo na palma de nossas mãos. O que falar, então, de conceitos como Internet of Things (IoT), Cyber Intelligence, Threat Intelligence, Cloud Computing, dentre outros.

Palavras-chave: IOT , Gateway, Anonimização.

INTRODUÇÃO

No cenário atual, o avanço das tecnologias digitais tornou-se um elemento essencial para a vida cotidiana, impactando diretamente a forma como interagimos com o mundo ao nosso redor. Contudo, essa crescente interconectividade também trouxe consigo desafios significativos para a privacidade e segurança, questões que se tornam ainda mais críticas no contexto militar. À medida que as operações cibernéticas ganham relevância, a anonimização e a proteção de dados sensíveis tornam-se vitais para a segurança nacional e a eficácia das operações de inteligência.

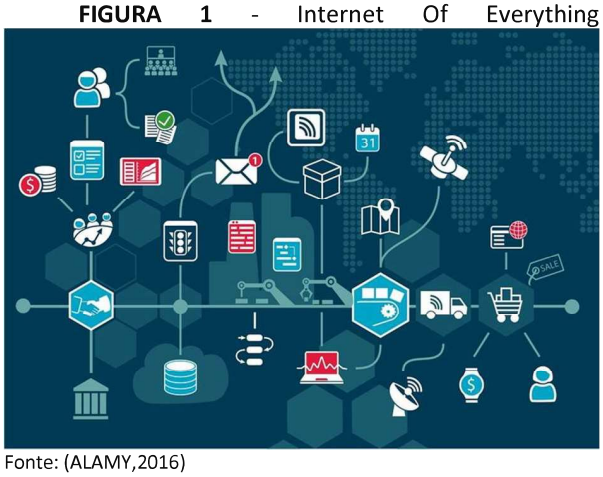
Este artigo aborda a continuidade de um projeto que visa aprimorar o uso de gateways de anonimização em operações militares, utilizando dispositivos de baixo custo como o Raspberry Pi. Explorando soluções para instabilidade de data e hora, além da implementação de VPN over TOR, o trabalho busca garantir que operadores militares possam realizar suas missões com maior segurança e anonimato, sem a necessidade de expertise técnica. A pesquisa e desenvolvimento contínuos são fundamentais para alcançar um estado da arte nesse campo e fortalecer as capacidades operacionais do Exército Brasileiro.

1. DESENVOLVIMENTO

1.1 A INTERCONECTIVIDADE E A DEPENDÊNCIA TECNOLÓGICA

O avanço tecnológico nas últimas décadas transformou profundamente a maneira como a humanidade interage com o mundo ao seu redor. A interconectividade, que antes era um conceito distante, agora é uma realidade onipresente que molda todos os aspectos da vida moderna. Dispositivos conectados, como smartphones, computadores e dispositivos IoT, tornaram-se extensões das atividades diárias, proporcionando acesso imediato a informações, comunicação e serviços de todas as partes do mundo.

FIGURA 1 - Internet Of Everything



Fonte: (ALAMY,2016)

No entanto, essa transformação não veio sem custo. A dependência dessas tecnologias é tamanha que, sem elas, é difícil imaginar manter a mesma qualidade de vida. As comodidades digitais, como o acesso rápido a notícias, a capacidade de realizar transações financeiras online e a comunicação instantânea, tornaram-se indispensáveis. Essa dependência criou uma sociedade em que a privacidade e a segurança são frequentemente sacrificadas em troca de conveniência.

Os computadores e dispositivos móveis, que armazenam informações pessoais, revelam uma quantidade impressionante de detalhes sobre os indivíduos. Esses dados vão desde preferências de navegação até informações de localização, que podem ser usadas para inferir hábitos, interesses e até padrões de comportamento. Cada página da web visitada, cada aplicativo utilizado, potencialmente expõe informações sobre a localização geográfica do usuário, os locais que ele frequenta e até as redes sociais que ele utiliza. Essa exposição contínua torna evidente a fragilidade da privacidade no mundo digital.

Essa nova realidade impõe um desafio significativo: como equilibrar a interconectividade com a proteção da privacidade e da segurança? À medida que a dependência tecnológica cresce, a necessidade de desenvolver e implementar soluções robustas de segurança torna-se cada vez mais urgente. A sociedade moderna precisa repensar sua relação com a tecnologia, buscando formas de preservar a privacidade e a segurança sem abrir mão dos benefícios que a interconectividade proporciona.

1.2 A SEGURANÇA EM UM CENÁRIO DE GUERRA CIBERNÉTICA

O avanço da tecnologia não apenas alterou a vida cotidiana, mas também redefiniu o cenário de conflitos e guerras. O ciberespaço emergiu como um novo teatro de operações, onde as fronteiras físicas são irrelevantes, e os ataques cibernéticos podem ser lançados de qualquer lugar do mundo. Diferente das guerras convencionais, onde o poder militar é medido pela força física e pela capacidade de destruição, as guerras cibernéticas são travadas no campo da informação e da tecnologia.

Um ataque cibernético bem-sucedido pode causar danos que ultrapassam em muito os impactos de um ataque cinético. Imagine um cenário em que uma infraestrutura crítica, como uma rede elétrica ou um sistema de transporte, seja comprometida por um ataque cibernético. As consequências podem ser catastróficas, afetando milhões de pessoas, paralisando economias e desestabilizando governos. A capacidade de um ataque cibernético de atingir alvos específicos, com precisão e sem necessidade de proximidade física, torna essa forma de guerra extremamente perigosa.

Nesse novo cenário, as forças armadas precisam adaptar suas estratégias para enfrentar as ameaças digitais. A defesa cibernética tornou-se uma prioridade, exigindo que as forças militares desenvolvam capacidades avançadas para proteger suas redes e infraestruturas críticas. Além disso, é necessário que essas forças sejam capazes de identificar e neutralizar ameaças cibernéticas antes que causem danos irreversíveis.

Para isso, a produção de conhecimento a partir de diversas fontes é essencial. As forças armadas devem estar sempre vigilantes, monitorando as atividades no ciberespaço e identificando potenciais ameaças. A inteligência cibernética, que envolve a coleta e análise de informações sobre possíveis adversários, é uma ferramenta crucial para a segurança nacional. As operações de segurança cibernética, por sua vez, visam proteger as infraestruturas e redes militares, garantindo que estas estejam sempre preparadas para resistir a ataques.

1.3 OPERATION SECURITY (OPSEC) E ANONIMIZAÇÃO

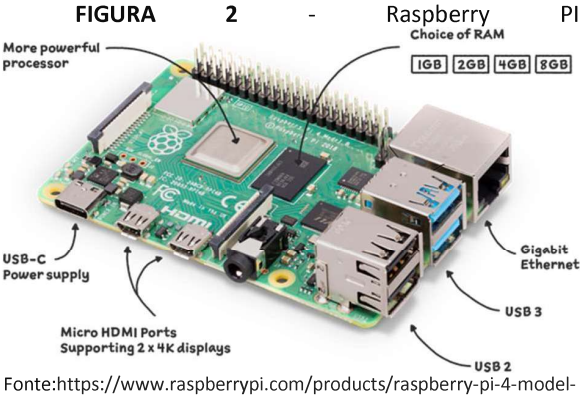
No contexto militar, a segurança da informação e a anonimização são

componentes críticos para o sucesso das operações. O conceito de Operation Security (OPSEC) é fundamental para garantir que informações sensíveis não caiam nas mãos erradas, protegendo as operações e os militares envolvidos. OPSEC envolve uma série de medidas e práticas destinadas a identificar e mitigar riscos de segurança, garantindo que informações vitais sejam mantidas seguras e fora do alcance de adversários.

A anonimização é uma parte crucial do OPSEC, especialmente em operações cibernéticas. No ciberespaço, onde a coleta de informações é uma prática comum, manter a privacidade e a segurança é um desafio constante. As operações militares que envolvem coleta de informações, compartilhamento de dados e comunicação precisam garantir que essas atividades sejam realizadas de forma anônima, para evitar rastreamento e identificação.

Projetos como o gateway de anonimização utilizando o Raspberry Pi, desenvolvido pelo 2º Sargento Lucas da Silva Lemes, exemplificam a importância de soluções tecnológicas acessíveis e eficazes para as forças armadas. Este projeto, que utiliza a rede TOR para permitir a navegação anônima, foi implementado pelo 1º Batalhão de Operações Psicológicas do Comando de Operações Especiais, mostrando-se uma ferramenta valiosa em operações de inteligência e operações especiais.

FIGURA 2 - Raspberry PI



Fonte:https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

Diante da necessidade de aprimorar e expandir essa solução, foram identificadas várias áreas para melhorias. Entre as principais, destaca-se a correção da instabilidade da data e hora do equipamento, que causava problemas na configuração e operação do gateway. Para resolver essa questão, foi implementado um módulo Real Time Clock (RTC), que garante que o dispositivo mantenha a hora correta, independentemente de sua conexão com a internet.

FIGURA 3 - Módulo RTC

Fonte:https://www.makerhero.com/produto/real-time-clock-rtc-ds3231/

Outra melhoria significativa foi a implementação da VPN over TOR, que adiciona uma camada extra de anonimização, garantindo que as comunicações sejam seguras e privadas. No entanto, desafios como a consulta a servidores DNS antes de passar pela rede TOR ainda precisam ser superados para que essa solução seja completamente eficaz.

Este projeto representa um passo importante na direção de fortalecer a segurança cibernética das forças armadas. Embora ainda existam desafios a serem superados, as melhorias implementadas até agora demonstram o potencial dessa solução para operações de inteligência e especiais. A continuidade desse trabalho é crucial para garantir que as forças armadas brasileiras estejam sempre preparadas para enfrentar as ameaças do ciberespaço, protegendo a soberania e a segurança nacional.

CONCLUSÃO

O avanço tecnológico e a crescente interconectividade trouxeram inúmeros benefícios para a sociedade, mas também apresentaram desafios complexos, especialmente no que diz respeito à privacidade e à segurança. No cenário militar, onde a proteção da informação e a anonimização são vitais, a adaptação às novas ameaças cibernéticas tornou-se uma prioridade. As guerras cibernéticas, que transcendem fronteiras físicas, exigem que as forças armadas desenvolvam estratégias sofisticadas para proteger suas operações e garantir a segurança nacional.

O conceito de Operation Security (OPSEC) e as práticas de anonimização destacam-se como elementos cruciais nessa nova fronteira de defesa. A implementação de projetos como o gateway de anonimização utilizando o Raspberry Pi demonstra a importância de soluções tecnológicas inovadoras e acessíveis para manter a segurança cibernética. As melhorias realizadas, como a correção da instabilidade da data e hora e a introdução de VPN over TOR, são passos significativos para o fortalecimento dessas operações.

No entanto, o trabalho está longe de ser concluído. A complexidade das ameaças cibernéticas requer uma abordagem contínua e evolutiva. A busca por soluções para desafios remanescentes, como a gestão de consultas DNS dentro de uma arquitetura de anonimização, é fundamental para consolidar a eficácia das ferramentas desenvolvidas. Portanto, é imperativo que este projeto e outros semelhantes continuem a ser aprimorados e adaptados às necessidades emergentes.

A continuidade das pesquisas e o desenvolvimento de novas tecnologias são essenciais para garantir que as forças armadas brasileiras possam operar com segurança e eficiência no ciberespaço. Somente através de uma abordagem proativa e inovadora será possível proteger a soberania nacional e garantir que o Brasil esteja preparado para enfrentar as ameaças do mundo digital.

REFERÊNCIAS

RASPBERRY PI 4. **Completely upgraded, re-engineered**. Disponível em: https://www.raspberrypi.com/products/raspberry-pi-4-model-b/. Acesso em: 30 agosto de 2024.

EXÉRCITO BRASILEIRO. **Manual de Campanha – Guerra Cibernética**. Brasília, 8 de junho de 2017.

BRASIL. MINISTÉRIO DA DEFESA. **Política Cibernética de Defesa**. Brasília, 21 de dezembro de 2012.

BROWSE PRIVATELY – **Explore Freely** Página inicial. Disponível em: https://www.torproject.org/. Acesso em: 05 julho 2024.

DEBIAN. **Documentação**. Disponível em: https://www.debian.org/doc/index.pt.html. Acesso em: 07 agosto 2024.

IP GEOLOCATION API. **Fast, accurate, reliable**. Disponível em: https://ip-api.com. Acesso em: 06 agosto 2024.

ROMERO, Mario Lobo. **Implementação de um dispositivo portátil de roteamento para redes anônimas baseado em Raspeberry Pi**. (Monografia de Especialização em Redes de Computadores e Teleinformática) – Universidade Tecnológica Federal do Paraná – UTFPR. Curitiba, PR, 2018. Disponível em: https://repositorio.utfpr.edu.br/jspui/handle/1/19974. Acesso em: 31 agosto. 2024.

TAILS. **Conectando à rede Tor**. Disponível em: https://tails.boum.org/doc/anonymous_internet/tor/index.pt.html. Acesso em: 28 agosto. 2024.

MAKER HERO. **Real Time Clock RTC DS3231**. Disponível em: https://www.makerhero.com/produto/real-time-clock-rtc-ds3231/. Acesso em: 31 agosto. 2024.

VIEIRA, Vinícius. **OPSEC. Inteligência Cibernética na prática**, 1ed, 2022.
The Tor Project. Disponível em: https://gitlab.torproject.org/legacy/trac/-/wikis/doc/TransparentProxy#local-redirection-and-anonymizing-middlebox. Acesso em: 31 agosto 2024