Proposta de Controles de Segurança Prioritários Contra-ataques em Redes Locais com Dispositivos Compactos

Paulo Victor de Araújo da Silva[1], Georges Daniel Amvame Nze[1], Fábio Lúcio Lopes de Mendonça[1], André Luiz Marques Serrano[1], Daniel Alves da Silva[1], Edna Dias Canedo[1]

vedgeta2@gmail.com, georges@unb.br, fabio.mendonca@unb.br, andrelms@unb.br, daniel.alves@redes.unb.br, ednacanedo@unb.br

[1] Universidade de Brasília (UnB), Campus Darcy Ribeiro, Departamento de Engenharia Elétrica, CEP 70910-900 Brasília-DF Brasil

Resumo: As estratégias de proteção para redes corporativas podem variar amplamente, abrangendo desde controles administrativos até técnicos. Identificar os controles mais adequados para tratar vulnerabilidades específicas é um desafio, especialmente diante de frameworks que listam dezenas ou até centenas de medidas. Este artigo, portanto, foca em uma forma particular de exploração de redes: as intrusões físicas por meio da inserção de dispositivos maliciosos nas redes-alvo. Essa técnica apresenta um alto impacto e representa um risco significativo para a continuidade dos negócios, pois explora vulnerabilidades que ultrapassam a segurança de perímetro. Com base em um estudo detalhado sobre esse tipo de ataque, este trabalho propõe um modelo de defesa em profundidade, estruturado com controles variados e priorizados para mitigar esse problema.

Palavras-chave: *Frameworks*, Intrusões Físicas, Segurança de Perímetro, Segurança em Profundidade.

Proposal for Priority Security Controls Against Attacks on Local Area Networks with Raspberry Pi

Abstract: Protection strategies for corporate networks can vary widely, ranging from administrative to technical controls. Identifying the most appropriate controls for specific problems is a challenge, especially when faced with frameworks that list dozens or even hundreds of measures. This article, therefore, focuses on a particular form of network exploitation: physical intrusions through the insertion of malicious devices into target networks. This technique has a high impact and poses a significant risk to business continuity, as it exploits vulnerabilities that go beyond perimeter security. Based on a

detailed study of this type of attack, this paper proposes a defense-in-depth model, structured with varied and prioritized controls to mitigate this problem.

Keywords: Framework; Physical Intrusions; Perimeter Security; Defense-in-depth.

1. Introdução

Nos últimos anos, os ataques cibernéticos têm evoluído significativamente, explorando vulnerabilidades não apenas pela Internet, mas também por meio de redes internas. Criminosos têm conseguido comprometer grandes organizações utilizando dispositivos compactos e de baixo custo, empregando técnicas furtivas, para evitar detecção, além de engenharia social, (Pankov, 2018).

Um caso emblemático ocorreu em 2018, quando a NASA foi invadida por meio de um *Raspberry* Pi, expondo dados sigilosos sobre missões espaciais e revelando falhas graves na gestão de inventário e detecção de dispositivos espúrios (Nogueira, 2019). Já em 2024, o Banco do Brasil registrou um prejuízo de R$ 40 milhões, após invasores instalarem dispositivos em cabos de dados e usarem engenharia social para corromper funcionários e acessar contas de correntistas (Leitão & Bruzzi, 2024). O Instituto Nacional do Seguro Social (INSS), autarquia do Governo do Brasil, também enfrentou ataques similares, reforçando a urgência de fortalecer políticas de controle de dispositivos e acessos (Pinheiro & Carone, 2023).

Assim, percebe-se que a priorização de controles de segurança diante de um cenário tão diversificado é um desafio, pois não há soluções universais que enderecem todos os riscos (NIST, 2020). Além disso, implementar múltiplos controles pode sobrecarregar operações e criar vulnerabilidades inerentes às novas contramedidas (ABNT 27005, 2018). Ainda, para escolha e implementação de controles, deve-se considerar o contexto em que o sistema esteja inserido e outras circunstâncias como obrigações regulatórias e políticas; a natureza das operações organizacionais; as funcionalidades específicas empregadas nos sistemas; processos negociais; interesses privados dos indivíduos; os tipos de informações processadas, armazenadas e transmitidas e; principalmente, o horizonte de ameaças enfrentadas por cada organização (NIST, 2020).

Diante disso, este artigo propõe um modelo para priorização de controles de segurança, utilizando a metodologia *Design Science Research* (DSR), com foco em prevenir, detectar e mitigar ataques com o uso de dispositivos compactos e furtivos.

O artigo está dividido em 6 partes: introdução que contextualiza brevemente o cenário estudado e expõe a relevância do tema; a seção 2 que introduz o referencial teórico e os trabalhos correlatos; a seção 3 apresenta a metodologia utilizada para desenvolvimento da proposta de controles; a seção 4 apresenta o desenvolvimento da proposta, análises e discussões sobre o resultado atingido, bem como dados sobre

um caso real de implementação de alguns controles para o problema; por fim, na seção 5, as conclusões deste trabalho e sugestões de trabalhos futuros.

2. Referencial Teórico

2.1. Trabalhos Correlatos

Segundo Asalqour et al. (2021), a implementação de um modelo bem estruturado de defesa em profundidade (*Defense in Depth*) é uma estratégia eficaz, pois envolve a aplicação de diferentes controles de segurança em camadas sucessivas, dificultando que técnicas complexas e variadas tenham sucesso em comprometer todas elas. A proposta do presente trabalho busca integrar controles focados na prevenção, detecção e mitigação do ataque estudado e suas variações, baseando-se nessa abordagem de segurança.

Thapa e Mailewa (2020) apresentaram uma revisão completa sobre a evolução histórica, funções e componentes dos sistemas de prevenção (IPS) e detecção de intrusão (IDS), além de listar as ferramentas mais utilizadas no mercado. Khraisat et al. (2019), por sua vez, trataram das abordagens contemporâneas desses sistemas, destacando técnicas de evasão usadas por atacantes, o que evidencia a constante evolução dos IDS nos últimos anos.

Em termos de segurança em redes internas, o protocolo IEEE 802.1x desempenha um papel crucial, fornecendo um mecanismo de autenticação para controlar o acesso de dispositivos às redes corporativas (IEEE, 2020). No entanto, Vishnu e Praveen (2020) destacam que sua versão mais básica apresenta fragilidades que permitem formas de contorno. La (2023) reforça a importância do processo de priorização de controles de segurança, reconhecendo que nem todos podem ou devem ser implementados, e sugere critérios como a probabilidade de ocorrência e as técnicas empregadas nos ataques como fatores determinantes na priorização.

Indo além de abordagens como defesa em profundidade ou o uso de IDS/IPS, o conceito mais amplo de *Zero Trust* parte da premissa de que nenhum participante da rede é confiável, independentemente de sua localização. Dessa forma, o *Zero Trust* busca garantir que todos os acessos sejam rigorosamente verificados em todas as camadas, redes e aplicações da corporação, substituindo a confiança baseada na localização por uma validação contínua e contextualizada (Arruda et. al., 2023).

Embora a literatura disponha de diversos estudos sobre tecnologias, conceitos ou controles específicos, bem como sobre a priorização de controles de segurança, este trabalho se distingue ao propor um modelo concreto de controles prioritários voltado para um problema específico que, além de ser complexo, afeta organizações de diferentes setores e tamanhos em escala global.

2.2. Priorização de Controles de Segurança

A priorização de controles de segurança é um tema amplamente discutido no campo da segurança cibernética. A publicação do NIST, SP 800-53, destaca que a seleção e priorização de controles de segurança deve ser guiada por uma análise de risco criteriosa, que avalie a criticidade dos ativos, as ameaças associadas e o impacto potencial dos ataques. Por esse motivo, o objetivo principal dessa abordagem é garantir que os controles estejam alinhados às necessidades organização, levando em consideração fatores como custo de implementação, eficácia na mitigação dos riscos e aderência aos requisitos regulatórios.

3. Metodologia

Este trabalho utiliza a metodologia Design Science Research (DSR), amplamente aplicada em pesquisas de sistemas de informação e engenharia. Seu objetivo é criar e avaliar iterativamente artefatos que solucionem problemas práticos enquanto geram contribuições científicas (Hevner et al., 2004). Este estudo adota o ciclo regulador de Wieringa (2014), uma abordagem iterativa da DSR que organiza as fases do desenvolvimento do artefato em ciclos de investigação do problema, projeto da solução, resultado e análises, conforme ilustrado na Figura 1.

Figura 1 – Ciclo de Wieringa (Adaptado de Wieringa)

Wieringa define o ciclo regulador para criação e avaliação de artefatos como um processo cíclico e contínuo, em que as fases se repetem até que uma solução satisfatória seja desenvolvida e validada. O ciclo adotado neste trabalho é uma versão adaptada desse modelo, estruturada em três fases principais:

- **Investigação do Problema**: O ciclo começa com a definição e descrição clara do problema prático a ser enfrentado. Essa etapa busca compreender,

com profundidade, o contexto e os fatores que originam a necessidade de intervenção (Wieringa, 2014).

- **Projeto da Solução**: Com o problema mapeado, o próximo passo é projetar o desenho da solução ou artefato. Neste estudo, com base nas diretrizes da NIST SP 800-53, foram revisados os controles de segurança capazes de mitigar, detectar ou prevenir diretamente o problema identificado (Wieringa, 2014).
- **Resultados e Análises**: Nesta fase do ciclo são realizadas Provas de Conceito (PoC) e analisados os resultados obtidos a partir da implementação dos controles descritos no modelo proposto. Nessa etapa, os controles são implementados e sua eficácia medida, até que se atinja o ponto ótimo entre custo de implementação e o valor do ativo a ser protegido (Wieringa, 2014).

4. Resultados, Análises e Discussões

Utilizando o ciclo de Wieringa da DSR, conforme metodologia proposta e utilizada neste trabalho, essa pesquisa foi desenvolvida de forma iterativa em que (1) se buscou entender o problema específico enfrentado, em seguida, (2) foi desenvolvida uma proposta de controles de segurança prioritários para endereçar o problema e, por fim, (3) foi avaliada a eficácia desses controles em um cenário prático. Em casos em que um controle não demonstrasse a eficácia esperada ou não pudesse ser aplicado ao cenário real, o ciclo foi repetido parcialmente, com o objetivo de refinar a solução e propor controles mais adequados e viáveis, mantendo o foco na efetividade e aplicabilidade prática.

4.1. Investigação do Problema – Como o Ataque Ocorre

O principal objetivo desse tipo de ataque é conectar e ocultar um dispositivo compacto na rede interna da organização-alvo e, criando uma ponte para que o atacante possa acessar remotamente a infraestrutura interna. Após o estabelecimento da conexão, o invasor pode apenas coletar dados trafegados ou credenciais utilizadas na rede, realizar movimentação lateral em direção a hosts legítimos da rede, escalar privilégio dentro desse ou outros dispositivos comprometidos e até mesmo tomar o controle do domínio, via *Active Directory*, por exemplo. Os dispositivos utilizados para esse tipo de ataque geralmente são roteadores compactos (3 polegadas de dimensão diagonal), como o Mikrotik HAP Mini, ou minicomputadores de baixo custo e alta versatilidade, como o *Raspberry* Pi. Esses dispositivos são facilmente adquiridos, discretos e capazes de executar funções avançadas de rede, o que os torna ideais para ataques furtivos. Conforme ilustrado na Figura 2.

Figura 2 - Mikrotik HAP Mini (esquerda) e *Raspberry* Pi (direita), ambos com medida aproximada de 3 polegadas de dimensão diagonal. Fonte: Mikrotik e *Raspberry* Pi.

A comunicação entre o atacante e o dispositivo espúrio pode ocorrer de diferentes formas, como por meio de uma conexão reversa pela própria rede da organização-alvo ou via acesso direto utilizando redes móveis 4G/5G, previamente configuradas no dispositivo. Scott Eggimann demonstra como preparar o dispositivo, por exemplo, instalando ferramentas e realizando a configuração da conexão reversa (*reverse shell*), que utiliza SSH (*Secure Shell*) nativo de sistemas Unix/Linux (Eggimann, 2022). Em sua análise, o autor destaca a grande quantidade de pontos de rede expostos em ambientes corporativos, que podem ser facilmente explorados por agentes maliciosos. Por sua vez, David Hunt, apresenta a possibilidade de utilização de servidores de comando e controle (C2) para controle remoto do dispositivo, além da utilização de outras ferramentas utilizadas para exploração de máquinas da rede do alvo, como Nmap, Metasploit e BurpSuite (Hunt, 2021).

Em consulta à matriz MITRE ATT&CK (MITRE, 2020), foi identificada a ocorrência de um grupo chamado "*Dark Vishnya*", número de identificação G0105, classificado como APT (*Advanced Persistent Threat*) com foco em ataques a instituições financeiras. APT ou Ameaça Persistente Avançada são adversários com níveis sofisticados de conhecimento e recursos significativos, geralmente patrocinados por governos (NIST, 2012). Segundo a *Kaspersky*, entre 2017 e 2018, o grupo atacou pelo menos 8 instituições financeiras naquela região da Europa. Entre as técnicas utilizadas pelo grupo, a mais notável é a inserção de dispositivos como *Raspberry Pi* ou outros tipos de laptops baratos (Pankov, 2018).

Ainda segundo Pankov, os ataques iniciavam com o (1) criminoso acessando o ambiente físico dos alvos, se fazendo passar por um visitante ou prestador de serviço; em seguida, (2) o dispositivo era inserido e ocultado em algum ponto da rede corporativa (Os pontos de rede, quase sempre, expostos em vários lugares dos escritórios corporativos como corredores e salas de reunião, onde visitantes, clientes

e parceiros são permitidos); após a inserção do dispositivo, (3) o atacante realizava acesso remoto à rede corporativa por meio de uma conexão celular 4G/5G, previamente configurada no dispositivo espúrio. Conforme ilustrado na Figura 3.

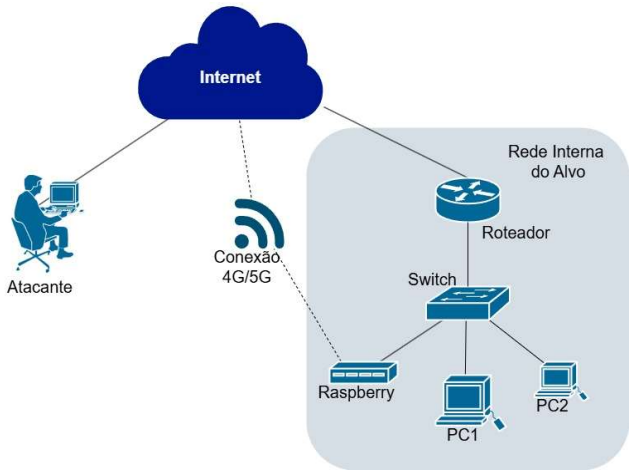

Figura 3 – Estrutura geral de uma intrusão em que se utilizam dispositivos compactos, como *Raspberry* Pi. Fonte: Autores.

Utilizando o dispositivo conectado à rede como estação de salto, os atacantes realizavam movimentação lateral e escalação de privilégios para persistir o acesso em outros pontos da rede. No Brasil, alguns ataques registrados repetiram essas formas de atuação e tinham objetivos similares (Bandeira, et al., 2023).

Na Figura 4, ilustra um caso real identificado em uma organização pública do setor financeiro no Brasil, que evidencia a replicação da estratégia utilizada pelo grupo *Dark Vishnya* em outros contextos ao redor do mundo. Nesse caso específico, um dispositivo Mikrotik HAP Mini foi conectado à rede interna da instituição e ocultado sob o piso elevado de uma das unidades da organização, reproduzindo fielmente as táticas de inserção discreta e persistência furtiva observadas nos ataques do grupo *Dark Vishnya*.

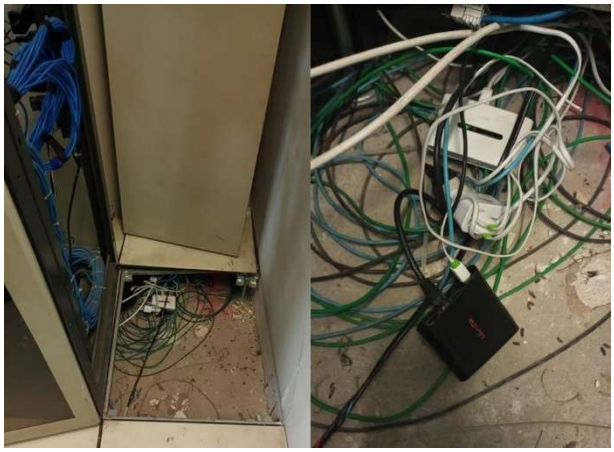

Figura 4 – Em um caso real, um dispositivo Mikrotik HAP Mini foi identificado oculto abaixo do piso elevado. Fonte: Autores.

A seguir, são discutidos de modo conceitual e formal os critérios utilizados para a seleção desses controles, bem como considerações que devam ser levadas em conta ao se adotar ou não as medidas sugeridas.

4.2. Proposta da Solução – Critérios para Definição da Adoção dos Controles

Para o desenvolvimento da proposta, foi escolhida a publicação especial NIST SP 800-53, revisão 5 de 2020, por se tratar de um dos guias mais abrangentes de controles de segurança atualmente disponíveis, reunindo uma ampla gama de domínios (NIST, 2020). Sendo assim, o framework do NIST foi adotado como fonte principal para seleção dos controles propostos neste trabalho. A partir dessa fonte, todo o *framework* foi avaliado de forma criteriosa, com o objetivo de identificar controles capazes de detectar, prevenir ou mitigar diretamente as ações descritas nos ataques apresentados na seção 4.1. Os controles selecionados passaram por um processo iterativo de análise e reavaliação, conforme o método DSR, de modo a garantir sua relevância frente ao cenário estudado.

O objetivo desta proposta é construir um modelo de controles prioritários (técnicos, administrativos e operacionais) para um problema específico, baseado no conceito de defesa em profundidade e que possam ser implementados em organizações de setores diversos. Dessa maneira, os controles devem compor uma abordagem multicamada e serem variados, focando em proteção de dados, aplicações, dispositivos, rede e perímetro (Mughal, 2018, pp. 1-20). Assim, foi possível compor uma relação de controles que atendam aos objetivos de proteção, detecção e

mitigação, considerando diferentes níveis de arquitetura e maturidade de segurança organizacional.

Controles como autenticação 802.1X, monitoramento de contas, inspeção de tráfego e inventário de dispositivos podem ser ajustados ao grau de criticidade e às exigências regulatórias de instituições financeiras, hospitais, plantas industriais, órgãos públicos, redes educacionais e empresas com filiais remotas. A adoção de uma arquitetura escalável e modular, ancorada em princípios de *Zero Trust*, permite implantar esses mecanismos conforme o risco e a maturidade de segurança de cada ambiente, criando modelos customizados para reforçar redes locais contra a inserção de dispositivos não autorizados e outras ameaças físicas.

A proposta de controles apresentada pode ser também adaptada a diferentes tipos e tamanhos de organizações ao adotar uma abordagem proporcional ao nível de risco e à capacidade de investimento. Em grandes empresas, por exemplo, é viável implementar medidas robustas como NAC, microssegmentação de rede, IEEE 802.1X e monitoramento contínuo com SIEM, enquanto pequenas e médias empresas podem se beneficiar de alternativas mais acessíveis, como bloqueio físico de portas, inventário de dispositivos, soluções *Open Source* de prevenção e detecção de intrusos e monitoramento básico de tráfego. Essa flexibilidade torna os controles aplicáveis em ambientes diversos — industriais, corporativos, educacionais, públicos ou privados e de pequeno a grande porte — permitindo que cada organização selecione e implemente medidas compatíveis com sua realidade operacional, colhendo benefícios concretos mesmo com recursos limitados.

Portanto, ressalta-se que a adoção de controles dentro do rol proposto deve ser adequada para cada cenário, considerando critérios como tamanho e complexidade da infraestrutura organizacional, exposição e tolerância a riscos cibernéticos, soluções já implementadas, orçamento disponível, quantidade de usuários, sensibilidade de dados, capacidade operacional, histórico de incidentes, tipo de tecnologias adotadas e parcerias em cadeia de suprimento.

4.2.1. Utilização do Risk Management Framework como Ferramenta Formal para Seleção dos Controles de Segurança

Em complemento a discussão conceitual de critérios da seção anterior, o *Risk Management Framework* (RMF), SP 800-37, revisão 2 de 2018, publicado pelo NIST, se apresenta como uma abordagem estruturada para a gestão de riscos e maior especificação na seleção de controles de segurança da informação com base em riscos identificados (NIST, 2018). Sua adoção se justifica pela possibilidade de integração nativa com o NIST SP 800-53, utilizada como base para a definição dos controles. Nesse sentido, o RMF fornece um processo formal composto por etapas estruturadas que incluem a categorização de ativos, seleção, implementação, avaliação e monitoramento contínuo de controles, permitindo sua aplicação a diferentes níveis de criticidade e maturidade em segurança.

Por ser agnóstico em relação a tecnologias, o RMF pode ser aplicado independentemente das soluções adotadas pela organização, o que permite sua utilização em ambientes heterogêneos (NIST, 2018). Sua estrutura é escalável, podendo ser adaptada a pequenas, médias e grandes organizações, com ou sem regulamentações específicas. Embora tenha sido idealizado para uso no setor público federal dos Estados Unidos, onde sua aplicação é obrigatória, o framework é amplamente recomendado para o setor privado, podendo ser implementado em instituições financeiras, redes educacionais, ambientes industriais, órgãos públicos ou empresas de tecnologia.

Portanto, como alternativa formal e estruturada, a adoção do RMF possibilita ainda mais refinamento na seleção de controles apropriados dentre os sugeridos neste trabalho. A estrutura do RMF oferece critérios formais para priorização com base no impacto e no contexto operacional, promovendo uma associação entre os riscos identificados e os controles a serem implementados. Assim, a aplicação deste framework contribui para que as medidas de segurança selecionadas estejam alinhadas à exposição ao risco, à criticidade dos ativos envolvidos e à capacidade de resposta da organização.

4.2.2. Definição dos Controles

Com base nos critérios discutidos na fase de projeto, foram selecionados 47 subcontroles ou aprimoramentos. Além dos critérios discutidos anteriormente, a justificativa para a escolha desses controles foi a capacidade de detectar, prevenir ou mitigar diretamente alguma das técnicas empregadas para consecução do ataque. Esses controles foram organizados conforme apresentado na Tabela 1, agrupando-os por sua natureza e sua relevância para os vetores identificados no cenário de ameaça descrito anteriormente:

Tabela 1 – Proposta Completa de Controles de Segurança

ID	Controles
AC-2 (g)	Monitorar o uso das contas.
AC-17 [1]	Empregar mecanismos automatizados para monitorar e controlar métodos de acesso remoto.
AT-2 (b)	Empregue técnicas para aumentar a conscientização sobre segurança e privacidade dos usuários.
AT-2 (d)	Incorporar em treinamentos as lições aprendidas com incidentes ou violações de segurança internas ou externas.
AT-2 [2]	Fornecer formação sobre como reconhecer e reportar potenciais indicadores de ameaça interna.
AT-2 [5]	Fornecer formação sobre a ameaça persistente avançada.

CA-7 (e)	Correlação e análise de informações geradas por avaliações de controle e monitoramento.
CA-8 [1]	Empregar um agente ou equipe de teste de penetração independente para realizar testes de penetração no ambiente.
CA-8 [2]	Empregar exercícios de *redteam* para simular tentativas de adversários de comprometer os sistemas e ambientes organizacionais.
CA-8 [3]	Empregar um processo de teste de penetração que inclua tentativas de contornar os controles associados aos pontos de acesso físico à instalação.
CA-9 (a)	Autorizar conexões internas ao ambiente apenas de componentes definidos pela organização.
CM-7 (b)	Proibir ou restringir/desabilitar o uso de funções, portas, protocolos, software e/ou serviços restritos.
CM-7 [9] (b)	Proibir o uso ou conexão de componentes de hardware não autorizados.
CM-8 (a)	Desenvolver e documentar um inventário de componentes do sistema que reflita com precisão o ambiente.
IA-2 [1]	Implementar autenticação multifator para acesso a contas privilegiadas.
IA-2 [2]	Implementar autenticação multifator para acesso a contas não privilegiadas.
IA-3	Identificar e autenticar dispositivos definidos pela organização antes de estabelecer uma conexão de rede.
IA-3 [1]	Identificar e autenticar dispositivos | Autenticação de rede Bidirecional.
IA-5 [1] (b)	Verificar, quando os usuários criam ou atualizam senhas, se as senhas não são encontradas na lista de senhas comumente usadas, esperadas ou comprometidas em bases de senhas vazadas.
IA-5 [1] (c)	Transmitir senhas somente através de canais protegidos com criptografia.
IA-5 [1] (d)	Armazenar senhas usando uma função aprovada de derivação de chave com sal, de preferência usando um *hash* codificado.
IR-2 [3]	Fornecer treinamento de resposta a incidentes sobre como identificar e responder a uma violação, incluindo o processo da organização para relatar uma violação.
IR-4 (a)	Implementar capacidade de tratamento de incidentes que seja consistente com o plano de resposta a incidentes e inclua preparação, detecção e análise, contenção, erradicação e recuperação.
IR-4 [5]	Implemente um recurso para desabilitar automaticamente um recurso caso violações de segurança sejam detectadas.
IR-6 (a)	Requisitar que o pessoal relate suspeitas de incidentes à resposta organizacional a incidentes.

IR-9 (d)	Isolar o sistema ou componente do sistema comprometido.
MA-5 (a)	Estabelecer um processo para autorização do pessoal de manutenção e manter uma lista de organizações ou pessoal de manutenção autorizado.
MA-5 (b)	Verifique se o pessoal não escoltado que realiza manutenção no sistema possui as autorizações de acesso necessárias.
MA-5 (c)	Designar pessoal organizacional com autorizações de acesso exigidas e competência técnica para supervisionar as atividades de manutenção de pessoal que não possua as autorizações de acesso exigidas.
PE-2 (a)	Desenvolver, aprovar e manter uma lista de indivíduos com acesso autorizado às instalações onde o sistema reside.
PE-2 (b)	Emitir credenciais de autorização para acesso às instalações.
PE-3 (d)	Acompanhar visitantes e controlar suas atividades que exigem escolta e controle.
PE-3 [3]	Empregar guardas para controlar os pontos de acesso físico às instalações onde o sistema reside, 24 horas por dia, 7 dias por semana.
PE-3 [8]	Utilize vestíbulos de controle de acesso em locais dentro das instalações.
PE-6 (a)	Monitorar o acesso físico ao ambiente para detectar e responder a incidentes de segurança física.
PE-6 [1]	Utilizar alarmes de intrusão e equipamentos de vigilância.
RA-10 (a)	Estabelecer e manter um programa de *threat hunting* para procurar indicadores de comprometimento (IoC) nos sistemas organizacionais e Detectar, rastrear e interromper ameaças que escapam aos controles existentes.
SA-8 [18]	Implementar o princípio de segurança por design em canais de comunicação confiáveis do ambiente organizacional.
SC-7 [20]	Fornecer a capacidade de isolar dinamicamente o ambiente de outros componentes do sistema.
SC-8 [1]	Implementar mecanismos criptográficos para impedir a divulgação não autorizada de informações.
SC-26	Incluir componentes nos sistemas organizacionais projetados especificamente para serem alvo de ataques maliciosos para detectar, desviar e analisar tais ataques.
SI-4 (a) [1]	Monitore o sistema para detectar ataques e indicadores de ataques potenciais de acordo com os seguintes objetivos de monitoramento.
SI-4 (a) [2]	Monitore o sistema para detectar conexões locais e remotas não autorizadas.
SI-4 [1]	Conecte e configure ferramentas de detecção de intrusão
SI-4 [13] (a)	Analisar o tráfego de comunicações e os padrões de eventos do sistema.

SI-4 [13] (b)	Desenvolver perfis que representem padrões comuns de tráfego e eventos.
SI-4 [13] (c)	Usar os perfis de tráfego e eventos no ajuste dos dispositivos de monitoramento do sistema.

A partir da proposta completa de controles, é possível realizar uma seleção parcial e mais adequada ao cenário de cada organização. A seguir, é descrito um caso prático dessa adoção, bem como os resultados alcançados com essa implementação.

4.3. Resultados e Análises – Implementação em Caso Prático e Discussão dos Resultados

Esta seção apresenta e analisa os resultados obtidos com a implementação prática de parte dos controles propostos (Conforme Tabela 2) em um ambiente corporativo real. É importante ressaltar que cada caso exige adaptação na escolha dos controles constantes nessa proposta, conforme critérios de adoção de controles descritos na seção 4.2. Nesse sentido, com o objetivo de demonstrar a aplicabilidade e a eficácia da proposta em um contexto real, foram selecionados e implementados 20 subcontroles extraídos da lista apresentada neste trabalho. A aplicação prática ocorreu em uma empresa brasileira do setor financeiro, que havia sido alvo recorrente de ataques com dispositivos compactos e ocultos. Nesse contexto, foram adotados controles específicos, selecionados com base na análise de riscos do ambiente, histórico de incidentes e capacidade operacional da organização, conforme apresentado na Tabela 2.

Tabela 2 – Controles Implementados em um Ambiente Corporativo Real

ID	Controle Aplicado
AC-2 (g)	Monitorar o uso das contas de usuário: Monitoramento de horários, locais e dispositivos utilizados para login, feito com Active Directory e Azure Entra.
AC-17 [1]	Empregar mecanismos automatizados para monitorar e controlar métodos de acesso remoto: Utilização de Firewalls para monitorar conexões não autorizadas de entrada de saída de protocolos de acesso remoto, como SSH.
CA-7 (e)	Correlacionar e analisar informações geradas por avaliações de controle e monitoramento: Geração de regras SIEM para identificação de padrões de ataque como varreduras de rede.
CA-8 [1]	Empregar um agente ou equipe de teste de penetração independente para realizar testes de penetração no ambiente: Como forma de replicar e entender os ataques para escolher as contramedidas.
CA-8 [2]	Empregar exercícios de *redteam* para simular tentativas de adversários de comprometer os sistemas e ambientes organizacionais: Foi realizado exercício para realizar o ataque em departamento aleatório, para entender o comportamento dos colaboradores e das contramedidas de segurança.

CA-9 (a)	Autorizar conexões internas ao ambiente apenas de componentes predefinidos: Autenticação via padrão IEEE 802.1x, apenas de dispositivos legítimos.
CM-7 [9](b)	Proibir o uso ou conexão de componentes de hardware não autorizados: Portas de Switch em modo de bloqueio, em caso de não autenticação.
CM-8 (a)	Desenvolver e documentar um inventário de componentes do sistema que reflita com precisão o ambiente: Criação e gerenciamento do inventário por ferramentas como Zabbix e Active Directory SCCM. Essa medida é importante para garantir melhor visualização dos ativos legítimos em relação aos dispositivos espúrios.
IA-3	Identificar e autenticar dispositivos definidos pela organização antes de estabelecer uma conexão de rede: Reforço de configuração do Controle de Admissão à Rede (NAC) para admissão posterior.
IA-3 [1]	Identificar e autenticar dispositivos | Autenticação de rede Bidirecional: Autenticação 802.1x com EAP-TLS, utilizando certificados digitais e PEAP. Essa medida é importante para evitar sucesso de *spoofing* de endereços físicos.
IR-2 [3]	Fornecer treinamento de resposta a incidentes sobre como identificar e responder a uma violação, incluindo o processo da organização para relatar uma violação: Treinamentos rotineiros para times diversos, com reforço sobre as formas de reporte em caso de alarme.
IR-4 [5]	Implementar um recurso para desabilitar automaticamente um recurso caso violações de segurança sejam detectadas: Port Violation habilitado em caso de mais um endereço físico ser identificado em uma mesma porta de switch.
MA-5 (a)	Estabelecer um processo para autorização do pessoal de manutenção e manter uma lista de organizações ou pessoal de manutenção autorizado: Reforço nas políticas de acesso físico.
PE-2 (a)	Desenvolver, aprovar e manter uma lista de usuários com acesso às instalações onde o sistema reside: Acesso físico mais rigoroso com redefinição de políticas.
PE-3 (d)	Acompanhar visitantes e controlar suas atividades que exigem escolta e controle: Acesso físico mais rigoroso com redefinição de políticas.
PE-3 [3]	Empregar guardas para controlar os pontos de acesso físico às instalações onde o sistema reside, 24 horas por dia, 7 dias por semana: Acesso físico mais rigoroso, em ambientes críticos, com redefinição de políticas.
SC-7 [20]	Fornecer a capacidade de isolar dinamicamente o ambiente de outros componentes do sistema: Criação de listas de controle de acesso dinâmicas (dACL) para isolamento e contenção de dispositivos, em caso de violação de regras de segurança.
SI-4 (a) [2]	Monitorar o sistema para detectar conexões locais e remotas não autorizadas: Monitoramento via CISCO ISE + SIEM para monitoramento de limite de MACs conectados em conexões locais e conexões extranet.
SI-4 [1]	Conectar e configurar ferramentas de detecção de intrusão em um sistema de detecção de intrusão para todo o sistema: Uso de IDS para identificação de indicadores de comprometimento (IoC) pelo tráfego da rede.

SI-4 [13] (a)	Analisar o tráfego de comunicações e os padrões de eventos do sistema: Uso de IDS para identificação de indicadores de comprometimento (IoC) pelo tráfego da rede.

Após a realização de testes em ambiente controlado (laboratório), as medidas selecionadas foram implementadas em ambiente real entre agosto de 2023 e setembro de 2024. Durante o ano de 2023, foram identificados e recolhidos 30 dispositivos Mikrotik e *Raspberry* Pi, todos conectados, de alguma forma, à rede corporativa da organização. Esses incidentes ocorreram antes da implementação efetiva das medidas de controle propostas neste trabalho. Já em 2024, com os controles parcialmente implementados e operacionais, foi possível detectar 28 dispositivos similares, que não chegaram a estabelecer conexões efetivas com os ativos da organização, conforme ilustrado na Figura 6. Assim, embora não tenha havido redução significativa da quantidade de tentativas de intrusão, houve mitigação quase completa dos impactos dessas tentativas, de 30 para apenas 1 caso, ou 96,67%. Nesses casos, os dispositivos geraram apenas alertas nos sistemas de monitoramento, permitindo ações preventivas e respostas rápidas por parte da equipe de segurança. Houve apenas um caso de conexão bem-sucedida, no qual ocorreu roubo de credenciais e acesso não autorizado a sistemas internos. Apesar da gravidade do incidente isolado, os resultados indicam redução significativa da superfície de ataque e aumento da capacidade de detecção precoce, refletindo a eficácia dos controles adotados.

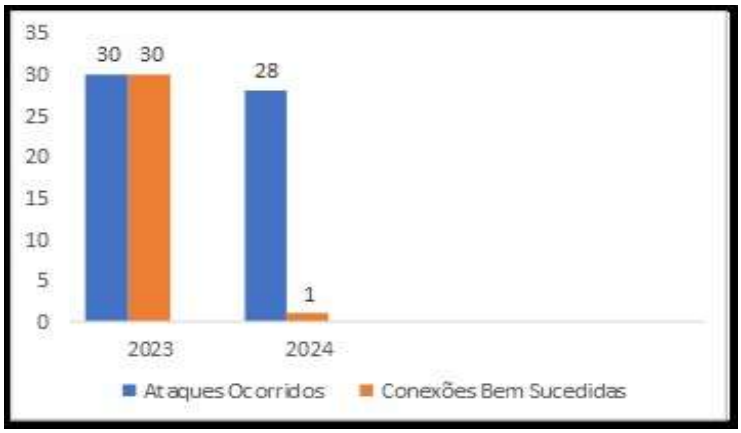

Figura 6 – Evolução de tentativas de ataque versus conexões bem-sucedidas, antes (2023) e após aplicação de controles de segurança (2024). Fonte: Autores.

Os resultados obtidos com a implementação real desses controles indicaram também impacto direto em indicadores como MTTR - *Mean Time to Respond* (Tempo Médio

de Resposta) e MTTD - *Mean Time to Detection* (Tempo Médio de Detecção), especialmente devido à maior automação e visibilidade introduzidas nos ambientes monitorados. Com a implementação dessas medidas em ambiente real, os incidentes deixaram de ser identificados, na maioria dos casos, após dias ou até semanas — quando a detecção dependia exclusivamente da identificação visual desses dispositivos espúrios conectados à rede — para serem detectados em tempo quase real. Essa evolução foi viabilizada, principalmente, (1) pela adoção de ferramentas automatizadas de detecção de dispositivos não autorizados e bloqueio de portas de rede e (2) pela integração com uma plataforma SIEM. Esses avanços demonstram que mesmo medidas de baixo custo, quando bem estruturadas, podem elevar a capacidade de resposta a ameaças em redes locais.

5. Conclusões e Trabalhos Futuros

Considerando o cenário alarmante e crescente número de ataques que utilizam dispositivos compactos e furtivos, como os descritos neste trabalho, esta pesquisa desenvolveu uma proposta de controles de segurança prioritários, voltados ao tratamento específico desse tipo de ameaça, oferecendo um caminho mais estruturado e direcionado para organizações expostas a esse risco. Por fim, durante a execução do estudo, constatou-se que, ao reduzir o conjunto de controles a ser considerado, com base em critérios técnicos e operacionais, o processo de tratamento das vulnerabilidades se torna mais assertivo, eficiente e alinhado à realidade do ambiente analisado. Então, conclui-se que há necessidade de aprofundamento contínuo, dado que novas metodologias e variações de ataque são constantemente desenvolvidas. Com isso, a resposta a essas ameaças requer medidas específicas de identificação, mitigação e detecção, que devem ser atualizadas e ajustadas conforme o avanço do cenário de ameaças.

Como trabalhos futuros, sugere-se incrementar a proposta, testando e implementando outros possíveis controles como: Uso de mapas de calor para identificação de conexões 4G/5G para acesso remoto aos dispositivos maliciosos; Criação de inventário de dispositivos com base em outras técnicas, como *fingerprint* de dispositivos utilizando SNMP ou outro protocolo, por exemplo; Implementação de tecnologias ZTNA (*Zero Trust Network Access*) para maior controle do acesso aos recursos de rede.

6. Agradecimentos:

Os autores agradecem o apoio do Laboratório LATITUDE, da Universidade de Brasília, ao TED 01/2021 da Secretaria Nacional de Assistência Social – SNAS/DGSUAS/CGRS, ao TED 01/2021 da Procuradoria Geral da Fazenda Nacional – PGFN, ao Projeto SISTER City (Outorga 625/2022 – FAP/DF), ao Projeto

SISPRO-DF" (Outorga 497/2023 – FAP/DF), ao Decanato de Pesquisa e Inovação – DPI/UnB e a FAP/DF.

Referências

Alsaqour, R., Majrashi, A., Alreedi, M., Alomar, K., & Abdelhaq, M. (2021). Defense in Depth: Multilayer of Security. *International Journal of Communication Networks and Information Security*. 13(2). 242-248.

Arruda, L. G. S., Giozza, W. F., Nze, G. D. A., & Nunes, R. R. (2023). Implementação da Arquitetura Zero Trust: uma Revisão Sistemática de Literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação*. E56. 264-275.

Associação Brasileira de Normas Técnicas [ABNT]. (2018). Tecnologia da informação: Técnicas de segurança: Gestão de riscos de segurança da informação - NBR 27005.

Bandeira, A. B., Neumann, C., Silva, D. A., Nze, G. D. A., Serrano, A. L. M., & Mendonça, F. L. L. (2023). Modelo para Utilização de Fingerprints de Sistemas Operacionais (SO) para Identificar e Responder a Conexões não Autorizadas de Dispositivos IOT na Ausência de Controle de Admissão à Rede (NAC). *Conferências IADIS Ibero-Americanas Computação Aplicada e WWW/Internet*. Volume único. 27-34.

Eggimann, S. (2022, June 8). Rogue Raspberry Pi Exploit. *Medium*. https://medium.com/@wicked_picker/rogue-raspberry-pi-exploit-a5f769b784d1

Hevner, A., March, S.T., Park, J, & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*. 28(1). 75-105.

Hunt, D. (2021, April 5). Catch Me If You Can. *f33d by Prelude*. https://feed.prelude.org/p/catch-me-if-you-can

Institute of Electrical and Electronics Engineers. (2020). IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control in IEEE Std 802.1X-2020 (Revision of IEEE Std 802.1X-2010 Incorporating IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018). https://doi.org/10.1109/IEEESTD.2020.9018454

Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. *Cybersecurity*. 2(20). 1-22.

La, S. (2023). Prioritizing Cybersecurity Controls Based on the Coverage of Attack Techniques and Attack Probabilities [Master's thesis, ETH Zurich]. Research

Collection. https://www.research-collection.ethz.ch/handle/20.500.11850/627198

Leitão, L., & Bruzzi, M. (2024, 8 de julho). Operação mira quadrilha que hackeava agências bancárias no RJ. G1. https://g1.globo.com/rj/rio-de-janeiro/noticia/2024/07/08/operacao-mira-quadrilha-que-hackeava-agencias-bancarias.ghtml

MITRE. (2020). DarkVishnya. https://attack.mitre.org/groups/G0105/

Mughal, A. A. (2018). The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. *International Journal of Intelligent Automation and Computing*. 1(1). 1-20.

National Institute of Standards and Technology. (2012). Guide for Conducting Risk Assessments: NIST Special Publication 800-30, Revision 1. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2018). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy: NIST Special Publication 800-37, Revision 2. https://doi.org/10.6028/NIST.SP.800-37r2

National Institute of Standards and Technology. (2020). Security and Privacy Controls for Information Systems and Organizations: NIST Special Publication 800-53, Revision 5. https://doi.org/10.6028/NIST.SP.800-53r5

Nogueira, L. (2019, 20 de junho). Laboratório da NASA é hackeado com ajuda de um Raspberry Pi. Olhar Digital. https://dev.olhardigital.com.br/ciencia-e-espaco/laboratorio-da-nasa-tem-sistema-invadido-por-meio-de-um-raspberry-pi/

Pankov, N. (2018, December 6). DarkVishnya Attacks from Inside. *Kaspersky Daily*. https://www.kaspersky.com/blog/dark-vishnya-attack/24867/

Pinheiro, M., & Carone, C. (2023, 16 de maio). Hackers invadem sistema do INSS e geram prejuízo de R$ 1 bilhão. Metrópoles. https://www.metropoles.com/distrito-federal/na-mira/hackers-invadem-sistema-do-inss-e-geram-prejuizo-de-r-1-bilhao

Thapa, S., & Mailewa, A. (2020, April 28). The role of intrusion detection/prevention systems in modern computer networks: A review. *EasyChair Preprint*. https://easychair.org/publications/preprint/jMT5

Vishnu, V., & Praveen, K. (2020). Bypassing Wired Port Security. *International Journal of Recent Technology and Engineering (IJRTE)*. 8(6). 3293-3297.

Wieringa, R. J. (2014). Design Science Methodology for Information Systems and Software Engineering. Springer.