

V. 06, N.27 Jan./Jun. 2025

CYBERSEGURANÇA : PRINCIPAIS DESAFIOS ENFRENTADOS POR PEQUENAS E MÉDIAS EMPRESAS

CYBERSECURITY : MAIN CHALLENGES FACED BY SMALL AND MEDIUM ENTERPRISES

CIBERSEGURIDAD : PRINCIPALES DESAFIOS QUE ENFRENTAM LAS PEQUENAS Y MEDIANAS EMPRESAS

1

Diego Neuber

Universidade Norte do Paraná

ORCID – <https://orcid.org/0009-0001-6474-5218>

Resumo: Este artigo explora os principais desafios de cibersegurança enfrentados por pequenas e médias empresas (PMEs) no Brasil e no contexto global. A análise abrange aspectos comerciais, financeiros e estratégicos, oferecendo uma visão abrangente das dificuldades enfrentadas por essas organizações e propondo estratégias para mitigação de riscos.

Palavras-chave: Cybersegurança. Informação. Ataques. PMEs.

Abstract: This article explores the main cybersecurity challenges faced by small and medium-sized enterprises (SMEs) in Brazil and globally. The analysis covers commercial, financial, and strategic aspects, offering a comprehensive view of the difficulties these organizations face and proposing strategies for risk mitigation.

Keywords: Cybersecurity. Information. Attacks. SMEs.

Resumen: Este artículo explora los principales desafíos de ciberseguridad que enfrentan las pequeñas y medianas empresas (PYMEs) en Brasil y en el contexto global. El análisis abarca aspectos comerciales, financieros y estratégicos, ofreciendo una visión integral de las dificultades que enfrentan estas organizaciones y proponiendo estrategias para la mitigación de riesgos.

Palabras-clave: Ciberseguridad. Información. Ataques. PYMEs.

INTRODUÇÃO

Com o aumento exponencial das ameaças cibernéticas, as pequenas e médias empresas têm enfrentado dificuldades crescentes em proteger seus ativos digitais. Apesar de desempenharem um papel crucial na economia, muitas PMEs permanecem vulneráveis devido à falta de recursos, conhecimento especializado e infraestrutura de segurança robusta. Este

estudo tem como objetivo identificar os desafios mais significativos enfrentados por essas empresas e discutir práticas e soluções para enfrentá-los.

Os ataques cibernéticos atingem organizações de qualquer porte e segmento, desde multinacionais a órgãos governamentais. Entretanto, cibercriminosos procuram pelos alvos mais vulneráveis, e geralmente é onde as micro e pequenas empresas se encontram..

2

METODOLOGIA

A pesquisa baseou-se em uma revisão da literatura existente, complementada por estudos de caso e entrevistas com especialistas em cibersegurança. Além disso, foram analisados relatórios de incidentes cibernéticos envolvendo PMEs, buscando compreender padrões e tendências.

PRINCIPAIS DESAFIOS

Phishing e Engenharia Social

Ataques de phishing e engenharia social têm sido amplamente utilizados por cibercriminosos para enganar funcionários e obter acesso não autorizado a sistemas e dados empresariais. Por meio de e-mails falsos, mensagens de texto ou chamadas telefônicas, os atacantes exploram a confiança dos usuários para obter informações sensíveis. Esses ataques frequentemente resultam em roubo de identidade, vazamento de dados e comprometimento de sistemas críticos. Para minimizar os riscos, é essencial investir em treinamentos regulares que ensinem os funcionários a identificar essas ameaças, além de implementar tecnologias como autenticação multifator e ferramentas de detecção de phishing.

Malware e Ransomware

O malware continua a ser uma das maiores ameaças às PMEs, sendo o ransomware uma de suas variações mais destrutivas. Esses softwares maliciosos comprometem sistemas, criptografam dados e exigem resgate para a sua liberação. Além de causar perdas financeiras, esses ataques podem paralisar as operações e prejudicar a reputação empresarial. A mitigação passa pela utilização de soluções antivírus confiáveis, realização de backups regulares e criação de um plano de resposta a incidentes para restaurar a normalidade de forma ágil.

3

Medidas de Segurança Insuficientes

Muitas pequenas e médias empresas ainda operam com medidas de segurança inadequadas, como ausência de autenticação multifator, falta de treinamento para os funcionários e inexistência de políticas de cibersegurança estruturadas. Essas deficiências aumentam a exposição a ataques, resultando em perdas financeiras e interrupções operacionais. Para enfrentar esse desafio, é fundamental que as empresas invistam em tecnologias modernas, promovam a conscientização dos funcionários e realizem auditorias regulares para identificar e corrigir vulnerabilidades.

Restrições Orçamentárias

As limitações financeiras frequentemente impedem que PMEs invistam adequadamente em cibersegurança, deixando suas infraestruturas expostas a ataques. Com recursos reduzidos, muitas empresas acabam priorizando outras áreas, negligenciando sua proteção digital. Soluções de baixo custo, como ferramentas baseadas em nuvem, softwares de código aberto e a terceirização de serviços especializados, podem ser opções viáveis para mitigar essas limitações e aumentar o nível de proteção.

Conformidade Regulatória

O cumprimento de regulamentações, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, apresenta desafios significativos para as PMEs, que frequentemente carecem de conhecimento e recursos para implementar políticas adequadas. A não conformidade pode gerar multas, penalidades e perda de credibilidade junto a clientes e parceiros. Para lidar com essas exigências, as empresas devem se familiarizar com os requisitos legais e adotar práticas que garantam a proteção de dados e a conformidade com as regulamentações.

4

Ataques à Cadeia de Suprimentos

Vulnerabilidades na cadeia de suprimentos têm sido exploradas por cibercriminosos como porta de entrada para atingir pequenas e médias empresas. Esses ataques podem comprometer dados sensíveis, interromper operações e prejudicar relações comerciais. Para prevenir esse tipo de ameaça, é necessário implementar medidas de segurança em toda a cadeia de suprimentos, realizar avaliações de risco periódicas e estabelecer parcerias colaborativas com fornecedores e parceiros.

Falta de Profissionais Especializados

Muitas PMEs enfrentam dificuldades para contratar ou manter profissionais de cibersegurança devido aos custos elevados e à falta de entendimento sobre as necessidades específicas do setor. Essa lacuna pode ser parcialmente preenchida por meio de parcerias com fornecedores especializados ou pela capacitação de funcionários existentes para lidar com questões básicas de segurança digital.

DISCUSSÃO

Os desafios enfrentados pelas PMEs em cibersegurança são diversos e complexos, exigindo uma abordagem integrada e estratégica. O aumento da organização dos cibercriminosos, combinado com a rápida evolução das ameaças, exige que as empresas invistam continuamente em soluções tecnológicas, capacitação de funcionários e parcerias com terceiros. Além disso, a conscientização sobre a importância da cibersegurança deve ser fomentada em todos os níveis organizacionais.

Associações como a Information Sharing and Analysis Organization (ISAO) podem fornecer inteligência valiosa sobre ameaças e apoiar as PMEs na construção de defesas mais robustas. A constante atualização das estratégias de cibersegurança, aliada ao uso de soluções acessíveis, é fundamental para fortalecer a resiliência dessas empresas em um ambiente de ameaças dinâmicas.

CONCLUSÃO

As PMEs enfrentam desafios significativos na proteção de seus ativos digitais. O sucesso na mitigação desses riscos depende da implementação de medidas de segurança robustas, da educação contínua dos funcionários e da colaboração com terceiros. Diante de um cenário de ameaças em constante evolução, é imperativo que as PMEs adotem uma postura proativa, revisem regularmente suas estratégias de cibersegurança e invistam em tecnologias e práticas que garantam a proteção de seus negócios.

REFERÊNCIAS

Agência Nacional de Proteção de Dados (ANPD). "**LGPD: Lei Geral de Proteção de Dados.**" Disponível em: www.gov.br/anpd

Cybersecurity & Infrastructure Security Agency (CISA). "**Cyber Guidance for Small Businesses.**" Disponível em: www.cisa.gov

Symantec. "The Evolution of Ransomware: Threat Intelligence Report." Disponível em: www.symantec.com

ISAO Standards Organization. "Information Sharing and Analysis for Small Businesses." Disponível em: www.isao.org