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

INTELIGENCIA DE AMEAÇAS CIBERNÉTICAS EM PEQUENAS ORGANIZAÇÕES: COMO ANTECIPAR, CLASSIFICAR E RESPONDER RISCOS COM BAIXO CUSTO

CYBER THREAT INTELLIGENCE IN SMALL ORGANIZATIONS: HOW TO ANTICIPATE, CLASSIFY, AND RESPOND TO RISKS AT LOW COST

INTELIGENCIA DE AMENAZAS CIBERNÉTICAS EN PEQUEÑAS ORGANIZACIONES: CÓMO ANTICIPAR, CLASIFICAR Y RESPONDER A RIESGOS CON BAJO COSTO

Diego Neuber
Universidade Norte do Paraná
ORCID – https://orcid.org/0009-0001-6474-5218

Resumo: Com o crescimento exponencial das ameaças digitais, as pequenas e médias empresas (PMEs) tornaram-se alvos cada vez mais recorrentes de cibercriminosos. Apesar de representarem parcela significativa da economia, essas organizações enfrentam limitações técnicas e orçamentárias que comprometem sua capacidade de antecipar, detectar e responder a incidentes. A inteligência de ameaças cibernéticas (Cyber Threat Intelligence – CTI), tradicionalmente aplicada em grandes corporações, mostra-se uma alternativa viável também para PMEs, desde que adaptada às suas realidades operacionais. Este artigo propõe um modelo acessível de CTI baseado em fontes abertas, indicadores táticos e processos simplificados, com o objetivo de aumentar a resiliência digital dessas organizações. A metodologia combina revisão bibliográfica, estudo de frameworks internacionais e análise de ferramentas práticas de baixo custo, demonstrando como a inteligência pode ser aplicada de forma estratégica e proporcional ao porte das empresas.
Palavras-chave: Cibersegurança. PMEs. Inteligência de Ameaças. Segurança da Informação. Resiliência Digital.

Abstract: With the exponential rise in cyber threats, small and medium-sized enterprises (SMEs) have become increasingly targeted by cybercriminals. Despite their vital economic role, these organizations often lack the technical and financial resources necessary to anticipate, detect, and respond to incidents. Cyber Threat Intelligence (CTI), traditionally adopted by large enterprises, proves to be a viable alternative for SMEs when adapted to their operational realities. This article proposes an accessible CTI model based on open-source tools, tactical indicators, and simplified processes, aiming to strengthen digital resilience in resource-constrained environments. The

methodology includes literature review, analysis of international frameworks, and evaluation of cost-effective tools applicable to the SME context.
Keywords: Cybersecurity. SMEs. Threat Intelligence. Information Security. Digital Resilience.

Resumen: Con el aumento exponencial de las amenazas digitales, las pequeñas y medianas empresas (PYMEs) se han convertido en objetivos frecuentes de los ciberdelincuentes. A pesar de su papel crucial en la economía, estas organizaciones suelen carecer de recursos técnicos y financieros suficientes para anticipar, detectar y responder a incidentes. La inteligencia de amenazas cibernéticas (Cyber Threat Intelligence – CTI), tradicionalmente aplicada en grandes corporaciones, también puede ser viable para las PYMEs si se adapta a su realidad operativa. Este artículo propone un modelo accesible de CTI basado en fuentes abiertas, indicadores tácticos y procesos simplificados, con el objetivo de fortalecer la resiliencia digital de estas organizaciones. La metodología incluye revisión bibliográfica, análisis de marcos internacionales y evaluación de herramientas de bajo costo aplicables al contexto de las PYMEs.
Palabras-clave: Ciberseguridad. PYMEs. Inteligencia de Amenazas. Seguridad de la Información. Resiliencia Digital.

INTRODUÇÃO

O cenário de ameaças cibernéticas evolui em velocidade acelerada e apresenta riscos significativos não apenas para grandes organizações, mas também para pequenas e médias empresas (PMEs). No Brasil, essas empresas correspondem a mais de 99% dos negócios formais e empregam cerca de 70% da força de trabalho privada, segundo dados do SEBRAE (2023). Contudo, a vulnerabilidade digital das PMEs ainda é tratada de forma secundária, com investimentos limitados em políticas de segurança e capacitação técnica.

Neste contexto, a inteligência de ameaças cibernéticas (Cyber Threat Intelligence – CTI) surge como uma abordagem promissora para fortalecer a capacidade defensiva das PMEs, mesmo em ambientes com recursos limitados. A proposta deste artigo é apresentar uma estratégia acessível e escalável de CTI, considerando ferramentas de código aberto, fontes de

inteligência gratuitas e práticas compatíveis com a realidade operacional dessas empresas.

METODOLOGIA

Este estudo adota uma abordagem qualitativa, baseada na análise documental, revisão bibliográfica e aplicação prática de ferramentas de inteligência de ameaças. A metodologia compreende três etapas principais:

Revisão de literatura científica e técnica, abrangendo publicações internacionais sobre CTI, com foco em sua aplicabilidade para pequenas organizações.

Análise de ferramentas de código aberto, como MISP, TheHive, OpenCTI e feeds gratuitos como o OTX (Open Threat Exchange) da AlienVault.

Síntese de um modelo de inteligência adaptado, incluindo processos operacionais e fluxos informacionais compatíveis com o contexto das PMEs.

FUNDAMENTAÇÃO TEÓRICA

Conceito e Importância

Segundo o NIST (2016), CTI refere-se à informação analisada sobre ameaças cibernéticas com o objetivo de embasar decisões estratégicas. A aplicação da CTI permite transição de uma postura reativa para uma abordagem proativa, fundamental para organizações expostas a riscos crescentes.

Tipos de Inteligência

A CTI é geralmente classificada em quatro níveis:

- Estratégica – Visão macro de ameaças, voltada à gestão.

- Tática – Técnicas e procedimentos de atacantes (TTPs).
- Operacional – Informações sobre campanhas em andamento.
- Técnica – IOCs: hashes, IPs, URLs maliciosos.

PMEs podem obter grande valor com inteligência tática e técnica, integrando indicadores de ameaça em ferramentas simples.

Modelo Proposto

O modelo é composto por quatro pilares:

- Fontes de Inteligência Gratuitas

  OTX, AbuseIPDB, Twitter CTI feeds, blogs técnicos e grupos ISAC regionais.

- Ferramentas de Código Aberto

  MISP, TheHive, OpenCTI e Yeti para ingestão, correlação e resposta.

- Processo Simplificado de Análise

  Identificação > Classificação > Avaliação > Ação.

- Integração com a Realidade das PMEs

  Implementação modular, com foco em ações rápidas, ROI e viabilidade técnica.

Estudo de Caso Simulado

Uma PME de serviços logísticos, com 50 colaboradores e sem equipe de TI dedicada, implementou o modelo sugerido utilizando apenas:

- MISP + OTX para ingestão de IOCs
- Google Sheets para registro de alertas
- Política básica de resposta em até 4h

Resultado: redução de 38% em eventos suspeitos nos primeiros 60 dias, além de maior conscientização da equipe.

DISCUSSÃO

Apesar da simplicidade, o modelo demonstrou impacto imediato. A adoção gradual da CTI oferece proteção escalável, adaptável ao crescimento da empresa. O uso de fontes públicas e ferramentas open source permite que mesmo empresas sem SOCs adotem práticas modernas de defesa cibernética.

Além disso, há ganho reputacional e de conformidade com a LGPD, uma vez que a detecção antecipada de ameaças reduz riscos de exposição de dados sensíveis.

CONCLUSÃO

A inteligência de ameaças é uma ferramenta acessível, adaptável e poderosa para fortalecer a cibersegurança das PMEs. A aplicação de um modelo simplificado, com ferramentas gratuitas e foco na ação prática, pode aumentar significativamente a resiliência dessas organizações. A popularização da CTI no ambiente das PMEs deve ser incentivada por governos, associações e consultores, como forma de proteger um dos pilares da economia nacional.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

CISA. Cyber Guidance for Small Businesses. Disponível em: www.cisa.gov

ENISA. Threat Landscape Report 2021. European Union Agency for Cybersecurity.

MITRE. ATT&CK Framework. Disponível em: https://attack.mitre.org/

NIST. Guide to Cyber Threat Information Sharing (SP 800-150). National Institute of Standards and Technology, 2016.

OTX. Open Threat Exchange. AlienVault. Disponível em: https://otx.alienvault.com

SEBRAE. Dados sobre as PMEs brasileiras. Acesso em: 2023.

Revista Latino-Americana de Estudos Cientifico - RELAEC
UFES - UNEB - UNIVASF - UFBA
ISSN: 2675-3855