Detecção de Anomalias com Machine Learning para Prevenção de Invasões em Redes Corporativas

Autor(res)

Felipe De Amorim Borba
Marco Antonio Ortiz Lima
Israel Pereira Silva
Bianca Carvalho De Oliveira
Lucas Torres De Brito Soares

Categoria do Trabalho

Trabalho Acadêmico

Instituição

CENTRO UNIVERSITÁRIO ANHANGUERA

Introdução

A transformação digital tornou os dados um dos principais ativos das organizações, integrando a tecnologia da informação ao seu funcionamento diário. A utilização de sistemas de gestão, muitos em ambiente de nuvem, trouxe maior eficiência, mas também ampliou os riscos de ataques cibernéticos ao expandir a superfície de ataque. Métodos tradicionais de segurança, baseados em assinaturas de ameaças conhecidas, têm se mostrado limitados diante de ataques cada vez mais sofisticados. Nesse contexto, a detecção de anomalias surge como uma alternativa importante, pois busca identificar comportamentos fora do padrão em uma rede, que podem indicar tentativas de invasão. O uso de algoritmos de Machine Learning se destaca por permitir a análise de grandes volumes de dados e a identificação de padrões complexos que seriam difíceis de perceber manualmente. Este trabalho tem como objetivo, analisar como as técnicas de ML vêm sendo aplicadas para detectar anomalias e auxiliar na prevenção de invasões em redes corporativas.

Objetivo

O objetivo deste trabalho é analisar a aplicação de Machine Learning na detecção de anomalias, comparando esta abordagem com os métodos de segurança tradicionais. Serão discutidas suas principais vantagens e os desafios na prevenção de invasões em redes corporativas.

Material e Métodos

Este trabalho foi desenvolvido a partir de uma revisão bibliográfica, com foco qualitativo e exploratório. A pesquisa utilizou artigos científicos e trabalhos acadêmicos recentes que tratam da aplicação de Machine Learning na área de Cibersegurança. As fontes foram escolhidas pela sua relevância no estudo de sistemas de detecção de anomalias, permitindo reunir e organizar informações que contribuíssem para os objetivos do estudo.

Resultados e Discussão

A análise da literatura mostra que os métodos tradicionais de cibersegurança, baseados em assinaturas de

ameaças conhecidas, são reativos e não acompanham a evolução dos ataques atuais. Fatores como a expansão do trabalho remoto ampliaram o "perímetro da rede", tornando as defesas convencionais ainda mais vulneráveis. Essa limitação se deve ao fato de não conseguirem detectar novas formas de ataque, como os ataques zero-day. A crescente complexidade das ameaças exige soluções mais adaptativas.

Nesse cenário, a detecção de anomalias com Machine Learning (ML) surge como uma alternativa proativa, sendo aplicada em ferramentas como Sistemas de Detecção de Intrusos (IDS) e firewalls adaptativos. Em vez de procurar apenas ameaças já catalogadas, os algoritmos de ML aprendem o comportamento normal de uma rede e identificam desvios que podem indicar invasões. Essa capacidade de analisar grandes volumes de dados e encontrar padrões complexos amplia a detecção de ataques que passariam despercebidos pela análise humana.

Entre as principais vantagens dessa abordagem está a possibilidade de reconhecer ameaças inéditas, como malware polimórfico e Ameaças Persistentes Avançadas (APT), sem depender de um banco de assinaturas. Além disso, o uso de ML contribui para reduzir a sobrecarga de alertas em equipes de segurança, automatizando tarefas rotineiras e permitindo foco em incidentes mais graves. Estudos também indicam que o uso de inteligência artificial pode reduzir custos de violações e acelerar a resposta a invasões.

Por outro lado, a aplicação de ML apresenta desafios significativos. O desempenho dos modelos depende diretamente da qualidade dos dados de treinamento; informações incorretas podem gerar falhas e aumentar os falsos positivos. Além disso, os próprios sistemas de IA são vulneráveis a "ataques adversariais", nos quais um invasor manipula os dados de entrada para enganar o modelo ou "envenena" o conjunto de treinamento para comprometer sua precisão. Outro obstáculo é a dificuldade de interpretar os resultados dos algoritmos, conhecida como o problema da “caixa-preta”, quando o sistema identifica uma ameaça, mas não explica de forma clara o motivo da decisão.

Conclusão

É possível concluir que a aplicação de Machine Learning na detecção de anomalias representa uma evolução significativa para a cibersegurança, superando as limitações dos métodos tradicionais. A capacidade de identificar ameaças desconhecidas de forma proativa é seu principal benefício. No entanto, desafios como a dependência de dados de qualidade, a interpretabilidade dos modelos e a vulnerabilidade a ataques adversariais precisam ser gerenciados. A eficácia dessa tecnologia depende, portanto, de uma abordagem equilibrada, que una inovação com uma implementação responsável.

Referências

MOREIRA, Andricson Abeline et al. Técnicas de ensemble learning para sistema de detecção de intrusão no contexto da cibersegurança. Revista de Segurança da Informação e Comunicação, v. 10, n. 1, p. 1-15, 2021.

MONFRE, G. A.; SILVA, F. G.; VICENTIN, A. C. Inteligência Artificial Aplicada à Cibersegurança: Soluções Estratégicas para um Ambiente Digital Resiliente.

BOECHAT, Gabriel Verleun. Análise da aplicação da inteligência artificial no atual cenário de cibersegurança.