13º SIEPE SALÃO INTERNACIONAL DE ENSINO, PESQUISA E EXTENSÃO
CIÊNCIA, TECNOLOGIA E INOVAÇÃO PARA UM PLANETA + HUMANO
17 a 19 nov.21

PROPOSTA DE UMA SOLUÇÃO INTEGRADA PARA ANÁLISE E MONITORAMENTO DE REDES

Mateus Oliva Soares, discente de graduação, Universidade Federal do Pampa, Campus Bagé
Marcelo Marchioro Cordeiro, discente de graduação, Universidade Federal do Pampa, Campus Bagé
Érico Marcelo Hoff do Amaral, docente, Universidade Federal do Pampa

mateusoliva.aluo@unipampa.edu.br

A segurança em ambientes de redes de computadores pode ser alcançada através de procedimentos realizados pelos especialistas da área, tendo como foco realizar a proteção dos dados contra ameaças externas, contudo, os baixos investimentos das organizações na área de segurança da informação resultam, consequentemente, o aumento de vítimas de crimes cibernéticos. Para um efetivo controle da rede é necessária a implementação de sistemas de monitoramento, os quais exigem o expertise do administrador destes ambientes. Dessa maneira, observa-se que o mercado de tecnologia conta com inúmeras ferramentas, as quais desempenham funções diferentes para a proteção de ambientes de rede, neste sentido, observar e analisar as informações geradas por tais ferramentas é primordial para evitar incidentes, porém o elevado número de dados gerados por estas soluções dificulta o processo de segurança. Desta forma, o presente estudo tem por objetivo realizar uma pesquisa sobre ferramentas simples para o gerenciamento de redes de computadores, com o foco na configuração destas, e como resultado propor um software de monitoramento integrado, com uma interface única e intuitiva, centralizando informações pertinentes sobre o tráfego de dados, com a emissão de alertas e respostas proativas (regras de firewall) aos incidentes de segurança em redes de computadores. O foco desta solução são empresas de pequeno e médio porte, que possuam equipes reduzidas de TI, sem departamentos específicos para a área de segurança de sistemas e da informação. Dessa maneira, realizou-se uma revisão teórica em periódicos da área de segurança cibernética, de modo a coletar informações sobre os principais softwares de monitoramento e segurança, protocolos utilizados e as principais métricas que devem ser observadas na administração da rede. A partir do referencial resultante, foi possível propor a arquitetura de um NOC (*Network Operations Center*), baseada nas ferramentas estudadas. Técnicas de engenharia de softwares foram também utilizadas para a modelagem desta arquitetura, por meio do levantamento dos requisitos funcionais, não funcionais, diagramas de casos de uso, classes conceitual e sequência. O resultado desta etapa possibilitou o desenvolvimento de um projeto-piloto, através do qual se identificou a viabilidade de utilização da solução proposta. A prototipação do software que ocorreu a partir de tecnologias integradas foram levantadas a partir dos estudos dos referenciais teóricos, linguagens de programação para desenvolvimento frontend e backend, assim como, a utilização de metodologias ágeis que propõe processos e ferramentas utilizados para o desenvolvimento de produtos e entregas contínuas. Portanto, observa-se a possibilidade uma integração de um software eficiente com a finalidade de monitorar as redes e implementação da vigilância dos hosts e, por conseguinte, possibilitar a identificação de incidentes e gerar notificações de alerta para os administradores. Entretanto, vale salientar ser necessária, posteriormente, a adição de ferramentas para prover novas funcionalidades para o protótipo, pois deverá, consequentemente, fornecer uma resposta ativa aos incidentes gerados

na rede. Diante dessa perspectiva, o software de monitoramento não deve ser a única ferramenta que as empresas utilizam para sua segurança, visto que outras estratégias de segurança devem ser seguidas em conjunto e, dessa forma, a empresa terá uma garantia de integridade de seus serviços. Logo, constata-se que a segurança e proteção da rede é proveniente de todos os usuários.

Palavras-chave: Monitoramento de redes; Segurança da informação; Softwares de monitoramento; Desenvolvimento.