

Utilização da Visualização da Informação Aplicada à Segurança de Redes

Luiz Felipe de Camargo,
José Remo Ferreira Brega
Universidade Estadual Paulista "Júlio de Mesquita Filho"
Bauru, Brasil
camargo.luizfelipe@gmail.com; remo@fc.unesp.br

Diego Roberto Colombo Dias
Universidade Federal de São João del-Rei (UFSJ)
São João del-Rei, Brasil
diegocolombo.dias@gmail.com

Resumo—Considerando a necessidade de se monitorar as redes de computadores modernas e o ganho de qualidade ao se utilizar técnicas de visualização, objetiva-se desenvolver uma ferramenta de monitoramento com ênfase no uso de recursos visuais. Para tanto, procede-se inicialmente com uma revisão sistemática do assunto. Desta forma, em tempo são observados os resultados preliminares provenientes das etapas iniciais da revisão, o que permite concluir que a continuidade do projeto é interessante, de modo a se obter as contribuições propostas.

Área: Sistemas de Informação

I. INTRODUÇÃO

Cada vez mais as redes de computadores estão integradas a vida das pessoas, sendo necessário que elas permaneçam sempre em pleno funcionamento. Entretanto, o monitoramento efetivo para garantir o funcionamento de uma rede, através de registro de todos os incidentes ocorridos, gera uma quantidade enorme de dados, causando problemas para o gerente de redes ao analisar e obter novas informações a partir desta. A fim de solucionar este problema, pode-se fazer uso das técnicas de visualização da informação, utilizando a visão humana para auxiliar a interpretação dos dados.

O propósito geral do trabalho a ser realizado é aplicar as técnicas de visualização da informação de maneira a obter uma ferramenta para monitoramento de redes que ofereça uma visão integrada dos diversos aspectos que compõe a situação de uma rede. Espera-se que o presente trabalho sirva como base de consulta para futuros pesquisadores interessados na área de visualização da informação aplicada a segurança e monitoramento de redes e que seja desenvolvida uma ferramenta funcional conforme proposto.

Em 2014 Kotenko e Novikova [1] utilizaram técnicas de visualização para manipular dados de segurança de domínios de rede com operação crítica. Guimarães [2] realizou um trabalho buscando classificar diversos estudos que utilizaram técnicas visuais para gerenciamento de redes e serviços, obtendo 285 artigos publicados entre 1985 e 2013. Também em 2016, Papadopoulos [3] realizou um estudo detectando, através de uma abordagem visual, anomalias de roteamento no protocolo BGP.

VII Workshop do Programa de Pós-Graduação em Ciência da Computação: "Interação entre Academia e Empresa", Unesp, Rio Claro, 14 e 15 de setembro de 2017.

A Seção 2 deste trabalho trata dos conceitos e técnicas utilizadas, seguida da Seção 3 que descreve a metodologia utilizada. Os resultados preliminares são apresentados na Seção 4. Por fim, tem-se as considerações finais.

II. CONCEITOS E TÉCNICAS

Segurança de informação é descrita como a proteção das informações de diversas ameaças que buscam colocar em risco a continuidade de um negócio. Através da segurança de informação se busca minimizar o risco decorrente destas ameaças, maximizando sempre o retorno sobre as oportunidades de negócio e investimentos [4]. A segurança está estruturada em três principais pilares: confidencialidade, integridade e disponibilidade. No entanto, podemos citar também outras propriedades: autenticidade, responsabilidade, não repúdio e confiabilidade. Os principais pilares são ilustrados na Figura 1.

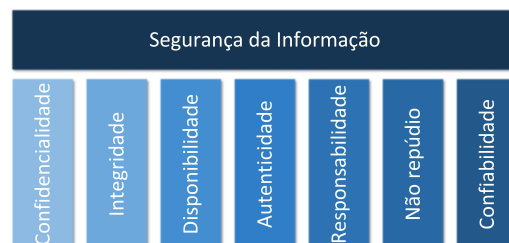


Figura 1. Os pilares da segurança de informação.

Monitoramento, o resultado do ato de monitorar, é definido por Michaelis [5] em seu dicionário da língua portuguesa como acompanhar e observar o decurso de um processo, de uma operação ou de um aparelho.

Gerenciamento de redes, segundo Saydam [6], pode ser definido como o processo que envolve o desenvolvimento, a integração e a coordenação de todos os recursos de hardware, software e de elementos humanos para monitorar, testar, configurar, analisar, avaliar e controlar uma rede, seus elementos e recursos para prover em tempo real os requisitos necessários de desempenho operacional e de qualidade de serviço a um custo razoável.

A visualização da informação busca representar conjuntos de dados como imagens, auxiliando na compreensão e tornando a interpretação destes mais eficiente. O uso da

Quais? — Por que? — Como?

(a) Identificação

Fonte	Contagem	Porcentagem
Engineering Village	92	43%
Scopus	67	31%
IEEE	42	20%
ACM	12	6%

(b) Seleção

Status	Contagem	Porcentagem
Duplicados	93	44%
Aceitos	64	30%
Rejeitados	56	26%