PROPOSTA DE UMA FERRAMENTA PARA MONITORAMENTO DE MÉTRICAS DE SEC-SLA NO CONTEXTO DA COMPUTAÇÃO EM NUVEM

Modalidade: ( ) Ensino (x) Pesquisa ( ) Extensão
Nível: ( ) Médio (x) Superior ( ) Pós-graduação
Área: ( ) Química (x) Informática ( ) Ciências Agrárias ( ) Educação ( ) Multidisciplinar

Autores: [1]Welligton ADÃO, [2]Alexandre AMARAL, [3]Ana Paula MALHEIRO.
Identificação autores: [1]Estudante do curso Sistema de Informação; [2]Orientador IFC *Campus* Camboriú; [3]Coorientadora IFC *Campus* Camboriú.

Introdução

A computação em nuvem tem se tornado imprescindível para os negócios das corporações de diversos nichos de atuação. Ela tem o potencial de reduzir os custos por meio da otimização e o aumento da eficiência no uso do *hardware* e *software* (Takabi *et al.*, 2010). No entanto, há riscos e diversas questões relacionadas a segurança e privacidade dos dados (Tariq *et al.*, 2013). Dentre eles estão o roubo ou modificações não autorizadas dos dados, ataques do tipo DoS (*Denial of sevice*) e proliferação de *malwares* (*malicious softwares*), dentre outros (Dali *et al.*, 2015; Guimarães *et al.*, 2016).

Para Takabi *et al.*, (2010) a principal preocupação dos usuários com respeito aos serviços de nuvem e o maior desafio dos provedores, refere-se a segurança e a privacidade. Assim, um acordo denominado Sec-SLA (*Security Service Level Agreement*) é firmado entre o cliente e o provedor de serviço de nuvem. Um Sec-SLA é um documento escrito que especifica os níveis de segurança que devem ser garantidos para o serviço contratado.

A fim de aferir se os parâmetros ou níveis de segurança estão sendo atendidos, *métricas* devem ser criadas (Putri e Mganga, 2011). O processo de criação e o monitoramento das métricas não é trivial, pois os aspectos de segurança (*e.g.*, privacidade dos dados) são inerentemente não quantitativos (Takabi *et al.*, 2010). Em função disso, muitos trabalhos têm sido propostos na literatura para viabilizar esse processo. No entanto, eles não têm discutido quais as fontes de dados que podem ser utilizadas para o monitoramento e quais os requisitos de um sistema para esse fim.

O objetivo desse trabalho é apresentar um protótipo de uma ferramenta gráfica contendo diferentes recursos úteis e necessários para o monitoramento de métricas Sec-SLA. Para isso, trabalhos de diversas áreas de conhecimento relacionadas à segurança da informação e de redes foram consultados. O trabalho tem o enfoque na discussão de quais os recursos e mecanismos que poderiam ser disponibilizados pelo sistema, para atuação no contexto da segurança na computação em nuvem.

Material e Métodos

Com o objetivo de propor uma ferramenta para o monitoramento de métricas Sec-SLA foi realizada uma busca em trabalhos da literatura relacionados à segurança da informação e redes. Além de trabalhos sobre e Sec-SLA e a computação em nuvem, outras áreas correlatas incluindo a de detecção de anomalias (Bhuyan *et al.*, 2014), detecção de intrusão (Dali *et al.*, 2015), correlação de alarmes (Sarkan *et al.*, 2015) e gerência de serviços e redes (Guimarães *et al.*, 2016) foram estudadas.

Em linhas gerais, baseado no que é apresentado na literatura, destacamos os seguintes itens para o desenvolvimento do sistema:

- **Sistema multiplataforma**: Possibilidade de ser instalado em diferentes sistemas operacionais e acessível a partir de diferentes dispositivos;
- **Funcionamento em tempo real**: Permitir que tanto o provedor quanto o cliente consigam interagir com os recursos de *hardware* e *software* disponíveis e/ou contratados, obtendo informações em tempo real (*e.g.*, gráficos dos incidentes de segurança) e relatórios;
- **Capacidade de detectar um maior número de ataques à segurança**: São necessários mecanismos capazes de detectar um maior número possível de incidentes de segurança. Além disso, é desejável que esses mecanismos de segurança sejam capazes de acompanhar as mutações e o surgimento de novas ameaças;
- **Tempo de resposta**: Atraso no diagnóstico do problema pode resultar em prejuízo financeiro para ambas as partes, principalmente para clientes que possuem serviços, cuja indisponibilidade é inaceitável, como as empresas administradoras de cartão de crédito;
- **Facilidade do entendimento do problema ocorrido**: Diz respeito ao meio utilizado para que as violações detectadas sejam apresentadas ao administrador e comunicadas ao cliente, permitindo um rápido entendimento e diagnóstico do problema para que medidas de reparo sejam aplicadas (Zhang *et al.*, 2014).

Nesse trabalho foi utilizado o *template* AdminLTE[1] para a criação do protótipo da ferramenta. Esse *template web* é *open source* contendo painéis voltados para a administração e controle. Ele utiliza o *framework* Bootstrap[2] na estilização dos componentes HTML. A ideia do AdminLTE é de permitir e facilitar a personalização de painéis pré-criados pelos desenvolvedores. Várias páginas e exemplos são disponibilizados, permitindo adaptações para o contexto desejado. Essas são as principais motivações pela escolha do AdminLTE.

[1] AdminLTE Control Panel Template - https://www.almsaeedstudio.com
[2] Bootstrap - http://getbootstrap.com

Resultados e discussão

A seguir são apresentados alguns croquis da ferramenta. A Figura 1 mostra um fragmento do *dashboard* do lado do cliente. Acreditamos que este deve apresentar informações sucintas, descrevendo o atual cenário dos recursos contratados.

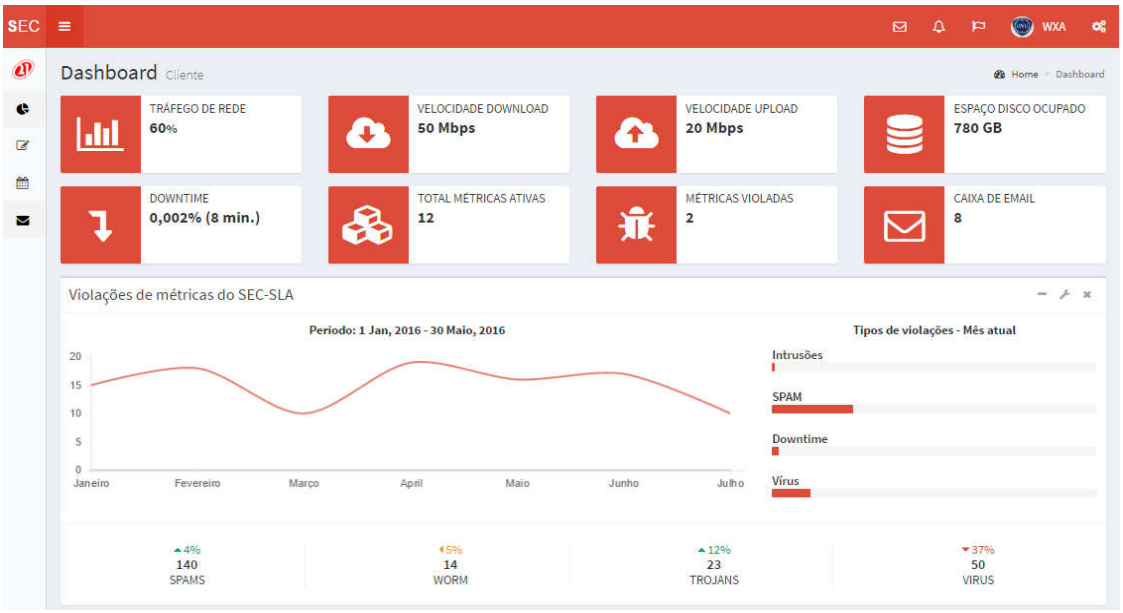

Figura 1. Protótipo de um *dashboard* do lado do cliente com informações sumarizadas dos recursos e métricas. Fonte: Autor.

Sob a perspectiva humana, a visualização gráfica é amplamente aceita como uma estratégia intuitiva para o entendimento do problema e a sumarização de dados (Zhang *et al.*, 2014). Em vez de gerar como resultado final inúmeros *logs* textuais, o sistema deveria permitir que tanto o administrador quanto o cliente interagissem diretamente com a visualização dos recursos disponíveis e alocados, tais como a utilização da rede (Figura 2, Figura 3), o espaço em disco (Figura 4), os tipos de dados trafegados pelo cliente (Figura 5), os servidores ativos/inativos e as falhas de *hardware* e *software*.

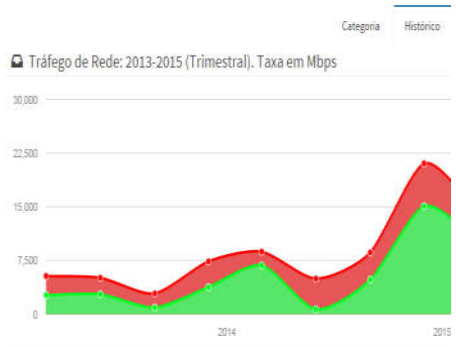

Figura 1. Medidor de banda de rede. Fonte: Autor.

Figura 2. Variação do uso de rede. Fonte: Autor.

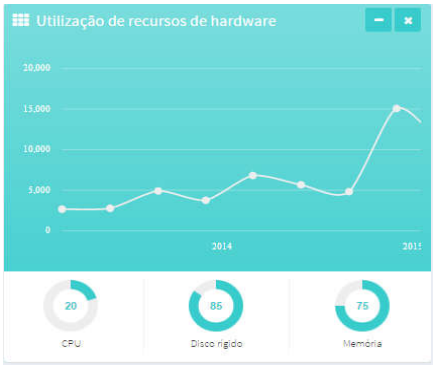

Figura 3. Contabilização do uso de recursos. Fonte: Autor.

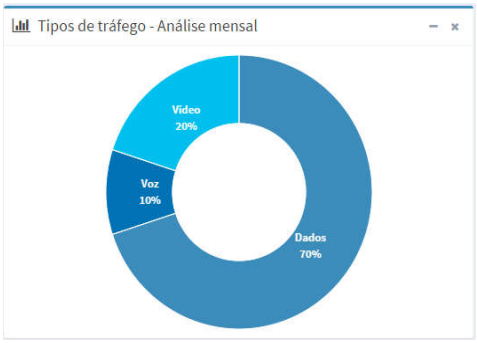

Figura 4. Tipos de dados trafegados na rede. Fonte: Autor.

Pelo aspecto da gerência das métricas, o sistema deveria de monitorar os diferentes tipos de métricas solicitadas pelo usuário, como mostra a Figura 6 (métrica para contabilizar o número de tentativas de intrusões, SPAM, *downtime* do servidor e vírus). Para isso o sistema precisaria processar diversas fontes de dados. Por exemplo, se uma métrica está relacionada a *Total de Anomalias de Redes Detectadas*, diferentes dados deveriam ser coletados para esse fim. Anomalias de redes envolvem uma miríade de possíveis problemas, incluindo os aspectos de falhas de *hardware* e *software* de rede, ataques (*e.g., brute force SSH*) e intrusões, e *malwares* como *worms* e trojans (Dali *et al.*, 2015).

Figura 5. Exemplo de gráfico representando métricas e violações. Fonte: Autor.

Não há uma fonte de dados panaceia. Por isso, para detectar os diferentes problemas, o sistema deve utilizar diversas fontes, tais como dados SNMP, fluxos IP (*e.g.*, NetFlow e IPFIX), *logs* de *firewall* (*e.g.*, Iptables) e proxy (*e.g.*, Squid), alertas de IDS (*Intrusion Detection System*) e IPS (*Intrusion Prevention System*), dentre outras (Nguyen e Choi, 2010). Essa heterogeneidade requer a normalização ou a padronização dos dados antes de serem analisados. É importante salientar também, que a fonte de dados disponível ou utilizada pelo

provedor delimita quais os tipos de métricas que poderão ser criadas e monitoradas. Além disso, o problema não reside apenas em qual o tipo de dado é o mais apropriado para monitorar uma determinada métrica, mas também outros fatores como a sua origem, qual o período que o dado será coletado e analisado (*e.g.*, a cada 5 min.) e como será armazenado (*e.g.*, banco de dados relacional ou NoSQL) (Bhuyan *et al.*, 2014).

Conclusão

Nesse trabalho foi proposto um protótipo de uma ferramenta gráfica voltada especificamente para o gerenciamento de métricas Sec-SLA. Discutimos as diferentes características e os principais requisitos considerados necessários para a atuação do sistema no contexto da computação em nuvem. Os desafios para atender esses requisitos também foram abordados. Como trabalho futuro estão o desenvolvimento da ferramenta e a sua utilização em um cenário real de um provedor de serviços de nuvem.

Referências

[1] BHUYAN, M. H.; BHATTACHARYYA, D. K.; KALITA, J. K., **Network Anomaly Detection: Methods, Systems and Tools**, in IEEE Communications Surveys & Tutorials, vol. 16, no. 1, p. 303-336, 2014.

[2] Dali L. et al., **A survey of intrusion detection system**, Web Applications and Networking (WSWAN), 2nd World Symposium on, Sousse, p. 1-6, 2015.

[3] NGUYEN, H; CHOI, D., **Network Anomaly Detection: Flow-based or Packet-based Approach?**. arXiv preprint arXiv:1007.1266, 2010.

[4] PUTRI, N. R.; MGANGA, M. C., **Enhancing Information Security in Cloud Computing Services using SLA Based Metrics**, School of Computing - Blekinge Institute of Technology, 2011.

[5] SARKAN, M. O.; AKÇAKOCA A.; KÜÇÜKAKDAĞ C.; ÇATALTEPE, Z., **Alarm correlation using Apriori algorithm**, 23nd Signal Processing and Communications Applications Conference (SIU), Malatya, p. 1602-1605, 2015.

[6] SILVA, C. A.; GEUS, P. L., **An approach to security-SLA in cloud computing environment**, IEEE Latin-America Conference on Communications (LATINCOM), Cartagena de Indias, p. 1-6, 2014.

[7] TAKABI, H.; JOSHI, J. B. D; AHN, G. J**., Security and Privacy Challenges in Cloud Computing Environments**, in IEEE Security & Privacy, vol. 8, no. 6, p. 24-31, 2010.

[8] TARIQ, M. I; HAQ, I. U.; IQBAL, J. **SLA Based Information Security Metric for Cloud Computing from COBIT 4.1 Framework**. International Journal Of Computer Networks And Communications Security, Dubai, v. 1, n. 3, p. 95-101, 2013.

[9] ZHANG, T.; LIAO, Q; SHI, L., **Bridging the Gap of Network Management and Anomaly Detection through Interactive Visualization**, IEEE Pacific Visualization Symposium, Yokohama, p. 253-257, 2014.