UMA ARQUITETURA HIERÁRQUICA MULTINÍVEL PARA CONSCIÊNCIA DE SITUAÇÃO EM SEGURANÇA DE AMBIENTES COMPUTACIONAIS

RICARDO BORGES ALMEIDA[1]; ROGER DA SILVA MACHADO[1]; DIÓRGENES YURI LEAL DA ROSA[1];LUCAS MEDEIROS DONATO[2]; ADENAUER CORREA YAMIN[1]; ANA MARILZA PERNAS[1]

[1]Universidade Federal de Pelotas – {rbalmeida, rdsmachado,adenauer, marilza}@inf.ufpel.edu.br, diorgenes.yuri@ufpel.edu.br
[2]De Montfort University – lucas.donato@myemail.dmu.ac.uk

1. INTRODUÇÃO

Tim Bass (1999) propôs a aplicação dos conceitos de Consciência de Situação (CS) no campo da segurança em redes de computadores, com o intuitode fornecer uma visão mais aprimorada dos aspectos de segurança do ambiente computacional. Tim Bass é tido como o primeiro autor a empregar estes conceitos na obtenção de um melhor entendimento sobre o ambiente monitorado.

Embora a união destas duas áreas venha sendo estudada há mais de dez anos, ela ainda constitui um foco de estudo e pesquisa relevante na área de segurança da informação (PESCATORE, 2015). Por sua vez, é importante registrar que devido ao crescimento em tamanho, distribuição e complexidade das redes de comunicação, as atuais soluções de segurança não têm se mostrado suficientemente efetivas na obtenção de uma visão integrada do ambiente computacional, apresentando limitações quanto à escalabilidade e flexibilidade (GHORBANI; LU; TAVALLAEE, 2010), (HU et al., 2014).

Neste cenário, é possível destacar alguns desafios particulares à obtenção da CS, como:o inerente uso de recursos distribuídos; a distribuição geográfica das organizações; a heterogeneidade dos ambientes no que diz respeito à coleta e tratamento dos eventos de segurança; e, a consequente dificuldade de monitoramento de dispositivos com este perfil operacional (PESCATORE, 2015).

Dentre os trabalhos existentes na literatura que abordam a aplicação da CS em segurança, (PREDEN et al., 2011) explora os conceitos de formação de hierarquias e de modelos de informação situacional com base em dados disponíveis a partir de um sistema de monitoramento distribuído de onde as propriedades temporais e espaciais de informação situacional são levadas em conta. Um estudo de caso é apresentadopara destacar a viabilidade dos conceitos em um cenário de monitoramento real.

O artigo (ZHANG et al., 2013) introduz um *framework* multinível de análises para a CS em segurança de rede como uma adaptação do modelo de Endsley (ENDSLEY, 1995). Não são apresentados detalhes sobre a proposta, aparentemente sendo um trabalho em desenvolvimento.

Em (TIMONEN et al., 2014), é apresentado um *framework* para a criação de um COP (*Common Operation Picture*) de infraestruturas críticas. O framework SACIN (*Situational Awareness of Critical Infrastructure and Networks*) demonstra as principais características do conceito. Como contribuições o trabalho destaca a combinação do modelo JDL (*Joint Directors of Laboratories*) e a arquitetura baseada em agentes. Neste artigo foram apresentados também os resultados dos testes realizados com os operadores do sistema.

Sente-se falta na nos trabalhos mencionados de aspectos pertinentes no emprego das soluções concebidas mapeadas sobre as infraestruturas

computacionais. Percebe-se também, a necessidade de uma arquitetura flexível e escalável, que atenda as demandas dos atuais ambientes computacionais.

Sendo assim, o presente trabalho apresenta como proposta a concepção de uma arquitetura hierárquica multinível para obtenção da CS sobre a segurança das infraestruturas computacionais, por meio de módulos que atuem desde o momento da coleta dos eventos, até seu processamento, armazenamento e projeção.

2. METODOLOGIA

A CS consiste da percepção e compreensão de uma ou mais informações contextuais e a projeção de seus efeitos em um futuro próximo. A percepção envolve os processos de monitoramento, detecção e reconhecimento, que levam a consciência de múltiplos elementos situacionais. A compreensão realiza a síntese e correlação dos elementos desconexos identificados na percepção por intermédio de diferentes estratégias. E por fim, a projeção é responsável pela capacidade de antecipação de ocorrências futuras(Onwubiko, 2012).

Desta forma, aCS será explorada no que tange a percepção devido à distribuição dos módulos de coleta de eventos, e da hierarquia multinível. A compreensão se dará pela seleção de uma estratégia de processamento de eventos de acordo com a necessidade do ambiente. Finalmente, a projeção, será fornecida no tratamento das situações de interessepelo emprego dos mecanismos de segurança previstos na infraestrutura de hardware e software dos equipamentos a serem protegidos.

A hierarquia será composta por componentes de softwareque consistem de uma entidade computacional autônoma, com uma máquina de estados que irá contemplar coleta de eventos, seu processamento considerando o modelo para consciência de situação empregado, o eventual disparo de procedimento de segurança, bem como quando necessário o repasse de informações para outros agentes localizados em nível superior da hierarquia.

3. RESULTADOS E DISCUSSÃO

A seguir, são descritos os componentes da arquitetura hierárquica multinível a ser concebida:

- Agente Local: cada dispositivo monitorado (inclusive os que hospedam agentes intermediários e o agente servidor) poderá possuir um agente local. Este agente será composto obrigatoriamente por estratégias de coleta de eventos (percepção), podendo opcionalmente realizar o processamento de eventos (compreensão) e a atuação sobre o ambiente (projeção). Este agente poderá coletar os eventos pertencentes ao dispositivo o qual ele é operacional, ou coletar eventos de tráfego da rede. Cada agente local poderá processar e repassar seus eventos para um ou mais agentes intermediários ou diretamente ao agente servidor, destacando a não obrigatoriedade da existência dos agentes intermediários. Caso algum dispositivo não possua capacidade de hospedar este componente, ainda será possível enviar os eventos do dispositivo por protocolos como Syslog ou *Simple Network Management Protocol* para o agente intermediário ou para o agente servidor.
- Agente Intermediário: visa filtrar e processar os eventos recebidos das camadas inferiores da hierarquia na procura por situações de interesse no que diz respeito ao seu escopo de visão e coordenação. Ele poderá

repassar seus eventos para outros agentes intermediários de maior nível, ou ao agente servidor.

- Agente Servidor: irá processar e armazenar os eventos recebidos de todo o ambiente analisado, fornecendo uma visão aprimorada e apoiando a obtenção da CS. Este agente poderá ser composto por diversos servidores para diminuir a sobrecarga e a existência de um único ponto de falha. Em qualquer nível da hierarquia é possível se ter um agente servidor para acesso das equipes de segurança no respectivo nível. Os diferentes servidores podem cooperar entre si para divisão da carga, podendo exigir algumas ações automatizadas de reconfiguração dos demais agentes. A filtragem nos diferentes níveis da hierarquia também auxilia na diminuição da carga dos agentes intermediários de níveis superiores assim como do agente servidor, além da redução do volume de tráfego.

Uma visão da hierarquia dos componentes que fazem parte da arquitetura para detecção de intrusão a ser concebida pode ser visualizada na Figura 1.

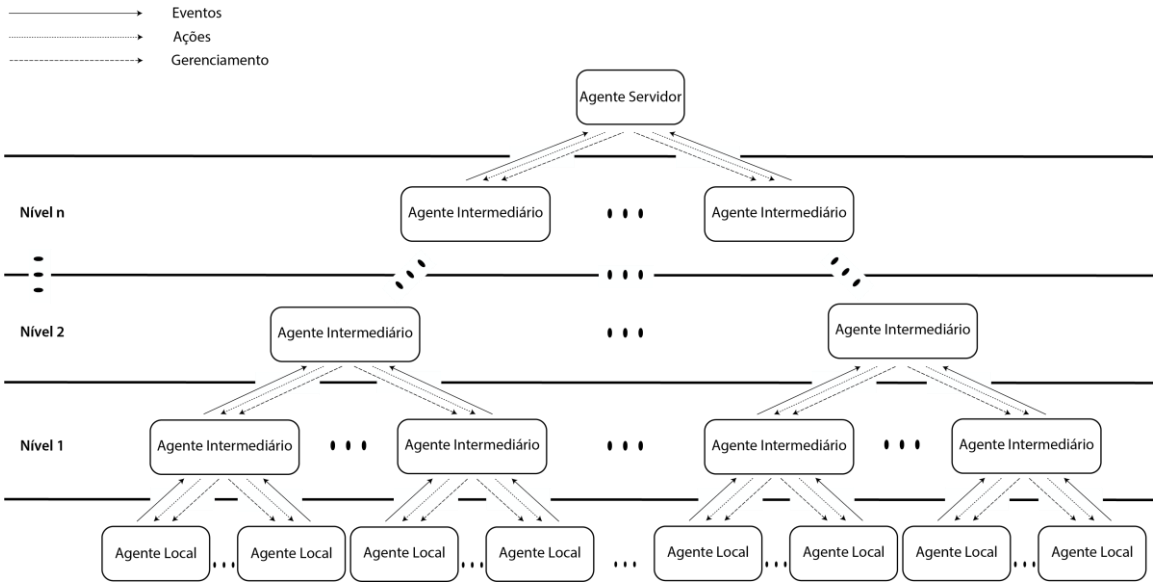

Figura 1 - Esboço da hierarquia dos componentes presentes na arquitetura

Os mecanismos de processamento disponíveis nos agentes podem envolver estratégias baseadas em anomalia e/ou em conhecimento. A definição das estratégias adotadas será influenciada pelas necessidades, imposições e recursos disponíveis da infraestrutura, fornecendo flexibilidade ao ambiente.

A realização de ações como consequência da projeção dos eventos coletados poderá ocorrer no próprio agente, ou de forma distribuída, como por exemplo, bloqueio no *firewall* de perímetro juntamente com o bloqueio no*firewall* de máquinas em Zona Desmilitarizada.

Ressalta-se que dependendodo ambiente distribuído observado, o número de níveis (compostos por agentes intermediários) necessários irá variar, podendo se resumir a agente local e agente servidor.

4. CONCLUSÕES

Como decorrência, por meio desta arquitetura, espera-se contribuir para a melhoria da obtenção da CS sobre a segurança em ambientes distribuídos, fornecendo: autonomia para os componentes da arquitetura localizados nos

diferentes nodos; flexibilidade para configuração, permitindo que módulos sejam habilitados ou desabilitados, de acordo com as necessidades e capacidades dos nodos envolvidos; escalabilidade, dando suporte ao crescimento vertical e horizontal da arquitetura para detecção de intrusão; e visibilidade da situação dos ambientes monitorados quanto às atividades maliciosas.

O uso da hierarquia multinível é o principal diferencial deste trabalho, visto que entre os trabalhos relacionados não foi identificado até o momento da escrita desta proposta uma abordagem similar.

A proposta será avaliada a partir de um cenário em que serão simulados ataques a arquitetura proposta. A arquitetura será implementada em um sistema distribuído que propicie a validação das principais contribuições buscadas no trabalho.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BASS, T. Multisensor data fusion for next generation distributed intrusion detection systems. **In Proceedings of the IRIS National Symposium on Sensor and Data Fusion**. Pages 24–27. 1999.

ENDSLEY, M. R. Toward a Theory of Situation Awareness in Dynamic Systems.**Human Factors: The Journal of the Human Factors and Ergonomics Society37**, 32-64(33). 1995.

GHORBANI, A.; LU, W.; TAVALLAEE, M. **Network Intrusion Detection and Prevention**: Concepts and Techniques. [S.l.]: Springer. (Advances in Information Security). 2010.

HU, W.; GAO, J.; WANG, Y.; WU, O.; MAYBANK, S. Online Adaboost-Based Parameterized Methods for Dynamic Distributed Network Intrusion Detection. **Cybernetics, IEEE Transactions on**, [S.l.], v.44, n.1, p.66–82, Jan 2014.

ONWUBIKO, C. Situational Awareness in Computer Network Defense: Principles, Methods and Applications: Principles, Methods and Applications. **Premier reference source. Information Science Reference**. 2012.

PESCATORE, J. Conquering Network Security Challenges in Distributed Enterprises. **Technical report, SANS Institute - InfoSec Reading Room**. 2015.

PREDEN, J., MOTUS, L., MERISTE, M., AND RIID, A. Situation awareness for networked systems. **In Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)**, 2011 IEEE First International Multi-Disciplinary Conference on, pages 123–130. 2011.

TIMONEN, J., PUUSKA, S., LÄÄPERI, L., VANKKA, J., AND RUMMUKAINEN, L. Situational awareness and information collection from critical infrastructure. **In Cyber Conflict (CyCon 2014)**,2014 6th International Conference On, pages 157–173. 2014.

ZHANG, H., SHI, J., AND CHEN, X. A multi-level analysis framework in network security situation awareness. **Procedia Computer Science**, 17, pages 530 – 536. First International Conference on Information Technology and Quantitative Management. 2013.