GERENCIAMENTO DE EVENTOS E INFORMAÇÕES DE SEGURANÇA: UMA ABORDAGEM EXPLORANDO A CONSCIÊNCIA DE SITUAÇÃO

RICARDO BORGES ALMEIDA[1]; ROGER DA SILVA MACHADO[1]; ADENAUER CORRÊA YAMIN[1]; LUCAS MEDEIROS DONATO[2], ANA MARILZA PERNAS[1]

[1]Universidade Federal de Pelotas, Centro de Desenvolvimento Tecnológico – {rbalmeida,rdsmachado,adenauer,marilza}@inf.ufpel.edu.br
[2]De Montfort University, Cyber Security Centre – lucas.donato@myemail.dmu.ac.uk

1. INTRODUÇÃO

O desenvolvimento de novas tecnologias da informação, bem como a evolução dos meios de comunicação e troca de dados, têm sido propiciados por diversas áreas de pesquisa, dentre estas destaca-se a Computação Ubíqua, idealizada por Mark Weizer (1991). Essas novas tecnologias estão cada vez mais integradas ao cotidiano das pessoas, nas comunicações, no setor financeiro e até no entretenimento. Infelizmente, todas as facilidades e potencialidades oferecidas por esta evolução também acabam sendo objeto de interesse de pessoas mal intencionadas, que usam destes recursos para cometer fraudes ou realizar ataques diversos contra sistemas de informação e/ou seus usuários. Logo, segurança e privacidade são desafios presentes na computação de forma geral que ficam potencializados na Computação Ubíqua devido à natureza volátil, espontânea, heterogênea e invisível de como ocorre a comunicação nos sistemas ubíquos (LANGHEINRICH, 2010).

A preocupação com a Segurança da Informação nas empresas tem aumentado nos últimos anos, e isto é consequência natural do aumento dos crimes realizados através da Internet e das perdas financeiras decorrentes. Somente em 2012, segundo relatório emitido pela Federação Brasileira de Bancos, R$1,5 bilhão foram gastos por conta de fraudes eletrônicas no Brasil (GOMES, 2012). Já o relatório do Instituto Ponemon aponta $8,9 milhões como custo médio anual originado pelo mundo do crime cibernético, representando um crescimento de 6% comparado a 2011 (PONEMON, 2012).

Atento a este cenário, o Instituto Ponemon, em seu relatório denominado "*The Risk of Insider Fraud: U.S. Study of IT and Business Practitioners",* destaca que 96% dos entrevistados consideram como uma das principais estratégias de combate à fraude interna - que representa em média 53% dos incidentes ocorridos em uma organização - a adoção de soluções de SIEM (*Security Information and Event Management* - Gerenciamento de Eventos e Informações de Segurança) (PONEMON, 2011). Ainda, de acordo com o Instituto, o custo do crime cibernético é mitigado pela utilização de sistemas de Segurança da Informação, pois empresas que utilizam tecnologias de inteligência de segurança (incluindo SIEM) foram mais eficientes na detecção e contenção de ataques cibernéticos. Como resultado, estas empresas obtiveram uma economia média anual de $1,6 milhão em relação às empresas que não implantaram tecnologias de inteligência de segurança (PONEMON, 2012).

Apesar de existirem excelentes soluções de SIEM, responsáveis por colocar esta categoria de solução em primeiro lugar em ambos relatórios do Instituto Ponemon, não foi encontrada uma SIEM com código fonte aberto e desenvolvida no meio acadêmico. Além disso, dentre as soluções FOSS (*Free and Open Source Software*) analisadas que realizam o tratamento de eventos, constatou-se que elas não utilizam os conceitos de consciência de situação, observando-se

que o emprego destes conceitos em soluções de SIEM tem se mostrado bastante oportuno, sendo explorado recentemente por soluções consolidadas disponíveis no mercado (MCAFEE, 2013).

Desta forma, o objetivo central deste trabalho é a concepção de uma solução de SIEM FOSS baseada no *middleware* EXEHDA (*Execution Environment for Highly Distributed Applications*) - visto que este *middleware* é voltado para Computação Ubíqua, área que potencializa os desafios relacionados à segurança de ambientes computacionais - focando na aplicação de consciência de situação à solução, através da correlação de eventos identificados por meio do monitoramento contínuo de logs e de informações sobre o estado do sistema, contemplando a diversidade de equipamentos que compõem a infraestrutura computacional ubíqua.

2. METODOLOGIA

A solução concebida, denominada SIEM-SA (*Security Information and Event Management - Situation Awareness*), é caracterizada principalmente pela capacidade de consciência de situação apoiada por um sistema de processamento de eventos. Além disso, a solução utilizou o *middleware* EXEHDA por ele possuir uma arquitetura distribuída que oferece suporte à aquisição, processamento e armazenamento de informações contextuais, além dos procedimentos de atuação sobre o meio, sendo estes fatores imprescindíveis para a obtenção de consciência situacional (YAMIN, 2004).

A concepção da solução utilizou os dois tipos principais de servidores presentes no EXEHDA: Servidor de Borda (SB) e Servidor de Contexto (SC). O SB é responsável pela interação com o meio através de sensores e atuadores, enquanto que o SC realiza o processamento das informações contextuais e o seu armazenamento no Repositório de Informações Contextuais (RIC).

A prototipação da solução objetivou o desenvolvimento de novas funcionalidades normalmente exigidas em uma solução de SIEM (CHUVAKIN, 2011) e o aprimoramento da segurança do próprio *middleware*, sendo destacadas a seguir:

- Configuração simplificada: visto que algumas soluções possuem um processo de implantação complexo, a configuração tanto do SB quanto do SC é realizada, primeiramente, através de um arquivo de configuração onde os parâmetros essenciais para inicialização são especificados, e posteriormente utilizando-se a interface Web;
- Dinamicidade de sensores: possibilita a ativação/desativação e inserção/remoção de sensores sem a necessidade de reinicialização do software presente no SB, evitando a perda de eventos pertencentes a sensores instanciados antes da modificação;
- Persistência local: esta funcionalidade, adaptada do EXEHDA, realiza a persistência local tanto das configurações dos sensores monitorados quanto dos eventos coletados e situações identificadas, destacando-se que os dados armazenados em memória e, posteriormente, em disco (caso o software seja finalizado) estarão criptografados;
- Desenvolvimento de novos *drivers*: a solução foi projetada de forma modular através de uma linguagem de alto nível (Python), o que colabora com a ideia de ser uma solução de código fonte aberto, e facilita o desenvolvimento de *drivers* para sensores ainda não suportados;

- Descoberta de recursos: visando a dinamicidade do hardware e das configurações dos dispositivos, principalmente na Computação Ubíqua, através da utilização de variáveis o sistema descobre os recursos que devem ser monitorados;
- Criptografia: para a comunicação entre o SB e o SC, a solução explora as vantagens tanto da criptografia por chave pública quanto da criptografia por chave simétrica desenvolvidas na camada de aplicação, além de utilizar a comunicação em XML-RPC (*Xtensible Markup Language - Remote Procedure Call*) através de conexões HTTPS (*HyperText Transfer Protocol Secure*);
- Consciência de Situação: é a identificação de situações de interesse, especificadas através de regras com sintaxe similar à SQL (*Structured Query Language*). Esta funcionalidade é realizada com o apoio de um sistema de processamento de eventos denominado Esper, e foi desenvolvida tanto no SB quanto no SC, propiciando uma Consciência de Situação distribuída e um aprimoramento da visão do ambiente através do módulo presente no SC;
- Tomada de ações: herdada do EXEHDA e aprimorada, é responsável pela execução de ações de acordo com as situações detectadas pelo módulo de consciência de situação. Exemplos de ações incluem o envio de *e-mails*, mensagens SMS (*Short Message Service*) e execução de comandos escritos em *shell script*, os quais podem atuar sobre o dispositivo ou sobre o meio.

Além destas funcionalidades, foi desenvolvida a capacidade de recebimento de eventos de diferentes dispositivos através do protocolo Syslog. Observa-se que, para o fornecimento destas funcionalidades, houve a necessidade de adequação do RIC.

3. RESULTADOS E DISCUSSÃO

O trabalho teve como resultado uma solução de SIEM FOSS com a capacidade de Consciência de Situação distribuída através da correlação de eventos. A seguir, a tabela 1 apresenta uma comparação do trabalho desenvolvido com algumas das principais soluções de SIEM do mercado (HP/ArcSight, IMB/Q1Labs, RSA/EM, Splunk e AlienVault) (GARTNER, 2013), acrescentando três soluções FOSS que realizam o tratamento de eventos.

Solução / Funcion.	HP/ ArcSight	IBM/ Q1Labs	RSA/ EMC	Splunk	OSSEC	SEC	AlienVault	SIEM-SA
FOSS	✗	✗	✗	✗	✓	✓	✓	✓
Consciência de Situação	✓	✗	✓	✓	✗	✗	✗	✓
Sintaxe ~SQL	✗	✓	✓	✓	✗	✗	✗	✓
Interface	✓	✓	✓	✓	✗	✗	✗	✓
Correlação Distribuída	✗	✓	✗	✗	✗	✗	✗	✓
Coleta com e sem agente	✓	✓	✓	✓	✓	✗	✓	✓

Tabela 1 – Comparação do SIEM-SA com soluções similares

Como contribuições decorrentes do trabalho desenvolvido, destaca-se:

- Minimização do tempo de possíveis respostas a incidentes, através da visualização dos eventos na interface Web, os quais são atualizados sem a necessidade de reinicialização forçada da página, conforme a inserção de novos eventos ocorrem no RIC. Além disso, a interface permite a aplicação de filtros;
- Diminuição de impactos adversos destes incidentes através da tomada de ações com base em situações detectadas;
- Garantia das evidências em investigações digitais, e também a criação de relatórios simplificados;
- Interface Web centralizada para apoio à auditoria;
- Monitoramento contínuo, que é descrito em guias de boas práticas e regulamentações.

4. CONCLUSÕES

O trabalho desenvolvido apresentou uma nova solução de SIEM, que se destaca por ser FOSS e utilizar os conceitos de Consciência de Situação através da correlação baseada em regras. A solução desenvolvida oferece uma interface Web, a qual permite a manipulação e a criação facilitada de regras a serem usadas para detecção de situações de interesse.

5. REFERÊNCIAS BIBLIOGRÁFICAS

CHUVAKIN, A. **The Complete Guide to Log and Event Management.** [S.l.]: Novell, 2011.

GOMES, H. Folha de São Paulo - Bancos perdem R$1,5 bilhão com fraudes. Disponível em: <http://www1.folha.uol.com.br/mercado/ 1161832-bancos-perdem-r-15-bilhao-com-fraudes.shtml>, acesso em: 03 abr 2013.

LANGHEINRICH, M. **Privacy in Ubiquitous Computing.** [S.l.]: J. Krumm, ed., CRC Press, 2010. 95-160p.

MCAFEE. **SIEM Requirements - Focus On Five.** 2013**.**

NICOLETT, M.; KAVANAGH, K. M. **Magic Quadrant for Security Information and Event Management.** [S.l.]: Gartner Group, 2013.

PONEMON. **The Risk of Insider Fraud:** U.S. Study of IT and Business Practitioners. [S.l.]: Ponemon Institute LLC, 2011.

PONEMON. **2012 Cost of Cyber Crime Study:** United States. [S.l.]: Ponemon Institute LLC, 2012.

WEISER, M. The Computer for the 21st Century. **Scientific American,** [S.l.], v.265, n.3, p.66–75, January 1991.

YAMIN, A. **Arquitetura para um Ambiente de Grade Computacional Direcionado às Aplicações Distribuídas, Móveis e Conscientes do Contexto da Computação Pervasiva.** 2004. Tese (Doutorado em Ciência da Computação) — Universidade Federal do Rio Grande do Sul.