ESTUDO E IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA PARA LOUSA ELETRÔNICA DO SISTEMA SHAVI

Alisson Lopes de Sousa Freitas (PIBIC/PIBIC-AF-IS/CNPq/FA/UEM), Luciana A. F. Martimiano (Coorientadora), Heloise Manica Paris Teixeira (Orientadora), e-mail: hmpteixeira@uem.br.

Universidade Estadual de Maringá / Centro de Tecnologia/Departamento de Informática/Maringá, PR.

Ciências Exatas e da Terra / Ciência da Computação

Palavras-chave: segurança da informação em saúde, lousa eletrônica.

Resumo:
O sistema SHAVI (*SHared VIew*) foi desenvolvido para atuar no setor de emergência do Hospital Universitário de Maringá-PR. O sistema provê o armazenamento e a gestão de informações das atividades desenvolvidas pela equipe de saúde do hospital, permitindo sua apresentação e compartilhamento em uma lousa eletrônica. Sistemas de informação na área de saúde gerenciam informações vitais para o tratamento de um paciente, portanto é fundamental planejar ações no sentido de garantir confidencialidade, integridade e disponibilidade das informações. Neste contexto, este trabalho implantou controles de segurança no sistema SHAVI, com vistas às recomendações ISO 27799:2008 e PoSIC/MS, que são voltadas para a área da saúde. Os controles implantados permitem controlar o acesso ao sistema, gerar e armazenar logs de auditoria, realizar backups e filtrar pacotes, garantindo características de segurança das informações.

Introdução

Em Sistemas de Informação em Saúde (SIS), em que os dados gerenciados devem ser confidenciais e íntegros, a implantação de mecanismos de segurança merece atenção. Deve ser planejada e realizada de maneira adequada, seguindo as melhores práticas e protocolos recomendados por organizações na área da saúde. Os SIS possuem dados e informações que devem ser mantidos em sigilo, pois são utilizados por especialistas no tratamento dos pacientes e para a tomada de decisão médica. A falta de confidencialidade, integridade e disponibilidade dos dados e informações pode levar a erros, dificuldades e atrasos no atendimento aos pacientes.
O manuseio de dados relacionados aos pacientes e seu atendimento devem seguir normas de segurança, que descrevem processos seguros para que os dados sejam armazenados, disponibilizados e transmitidos. A ISO 27799:2008 (ISO/IEC, 2008) é uma norma que define controles para apoiar a gestão da segurança nas organizações da área da saúde. Ela descreve várias recomendações, que devem ser seguidas tanto por desenvolvedores,

responsáveis pela implementação e manutenção de um SIS, como pelos usuários do sistema. Outra referência é a Política de Segurança da Informação e Comunicações do Ministério da Saúde (PoSIC/MS), regulamentada pela Portaria n°271, de janeiro de 2017 (BRASIL, 2017).
O sistema, denominado SHAVI (*SHared VIew*), está sendo desenvolvido com base no setor de emergência do Hospital Universitário de Maringá (HUM) e possui como principais funcionalidades o armazenamento e a organização das informações do trabalho realizado pela equipe de saúde para que possam ser apresentadas e compartilhadas em uma lousa eletrônica (ALMEIDA et al., 2014). O presente projeto tem como objetivos estudar e implementar uma política de segurança para o sistema SHAVI. Os resultados indicam que a implantação dos módulos de segurança contribuiu no sentido de melhorar a segurança e a confiança da informação utilizada para o atendimento de pacientes na unidade de emergência do hospital.

Materiais e métodos

Para o desenvolvimento da pesquisa, em uma primeira etapa foram estudadas as recomendações da ISO 27799:2008 e da PoSIC, e também o ambiente do hospital onde o sistema SHAVI será implantado.
Com base no estudo, foram implantados os seguintes módulos de segurança: controle de acessos, geração e armazenamento de *logs* de auditoria, *backups* e filtro de pacotes (*firewall*). Para cada módulo, foram estudadas diversas ferramentas e selecionada àquela que melhor atendesse aos requisitos de segurança do SHAVI e do ambiente em que ele será implantado. Para escolha de cada ferramenta, foram considerados fatores como desempenho, integração com a linguagem Java, facilidade de uso (configuração), custo (optou-se por ferramentas gratuitas), dentre outros.
Os softwares utilizados incluem a Linguagem de programação Java, o IDE Netbeans 8.0.2, MySqlBackupFTP, Uranium Backup e o Comodo Firewall.

Resultados e Discussão

O desenvolvimento dos módulos de segurança foi baseado nas recomendações da ISO 27799:2008 e da POSIC/MS. A Tabela 1 relaciona os principais controles desenvolvidos. A primeira coluna resume os principais controles de segurança que devem ser implementados em um sistema da área da saúde, a segunda descreve as características do controle implementado no sistema SHAVI e a terceira indica a ferramenta utilizada.

Tabela 1 - Controles X Implementação no SHAVI

Controle (ISO 27799:2008 e POSIC/MS)	Implementação no SHAVI	Ferramenta Utilizada
1. Implementar **backup** das informações.	Backup dos arquivos e do banco de dados.	Uranium Backup.

2. Implementar controle de **firewall**.	A prevenção, detecção e resposta de softwares maliciosos ficará à cargo de um software específico de *firewall*.	Comodo Firewall.
3. Criar **logs de auditoria**.	O registro dos eventos é realizado desde a entrada até a saída do usuário no sistema SHAVI.	Java.util.logging.
4. Implementar um **controle de acesso**.	O controle de acesso é baseado na função do usuário. Ou seja, é atribuída uma regra de acordo com a função ou o cargo no hospital.	Spring Security.
5. **Identificar** usuário/paciente de forma **única e segura**.	A identificação e autenticação do usuário são feitas no momento do *login*.	Spring Security.

De acordo com a norma (item 1 da Tabela 1), deve ser feito *backup* de todas as informações do SIS. A implementação do *backup* foi organizada em dois tipos: *backup* dos arquivos de auditoria e *backup* do banco de dados. Para o *backup* dos arquivos, foi utilizada a ferramenta Uranium Backup. Nela é possível fazer as principais configurações necessárias, como a escolha das pastas de origem e de destino, recebimento de notificações via e-mail, agendamento do *backup*, dentre outras. Na implementação do *backup* do banco de dados, foi utilizada a ferramenta MySqlBackupFTP. Com esta ferramenta é possível configurar quais bancos de dados serão considerados para o *backup*, selecionar a opção de enviar uma notificação por e-mail, agendar *backup*, dentre outras.

Outro controle indicado na norma (item 2 da Tabela 1) refere-se à implementação de controles para prevenção, detecção e resposta a softwares maliciosos. Na implementação do *firewall,* foi utilizada a ferramenta Comodo Firewall. Com a ferramenta é possível visualizar informações sobre as configurações de segurança atual, como por exemplo, a quantidade de intrusões na rede, quantidade de intrusões bloqueadas, executar a área de trabalho virtual, dentre outras.

A norma estudada também destaca a importância da criação de registro de auditoria sempre que um usuário acessar ou criar um arquivo (item 3 da Tabela 1). Esse registro deve identificar unicamente o usuário, identificar a função realizada pelo usuário e observar a hora e a data em que a função foi executada. A implementação dos *logs* de auditoria foi realizada em uma classe específica para tratar segurança no sistema SHAVI. Essa classe é responsável pela geração dos arquivos de auditoria, os quais são divididos em dois tipos: *logs* de acessos e *logs* individuais de cada usuário. Nos *logs* de acessos são armazenados dados dos usuários que logaram no sistema, tais como: nome, CPF, cargo, função utilizada e a data e o horário em que a função foi executada. Já os *logs* individuais são gerados para cada usuário de acordo com o seu cargo e com as seguintes informações: data, hora e a função que o usuário executou.

De acordo com a norma (item 4 da Tabela 1), para registrar e identificar um usuário do sistema de saúde é preciso: a captura precisa da identidade; a captura da credencial e/ou cargo; e a atribuição de um identificador. No

sistema SHAVI, o processo de autenticação e autorização do usuário é realizado no momento do seu *login*, e fica a cargo de um *framework* denominado Spring Security. Este *framework* é específico para o desenvolvimento da estrutura de controle de acesso, que é baseada em papéis ou grupos de usuários.

Conclusões

O desenvolvimento desta pesquisa foi de grande relevância no sentido de implantar controles de segurança no sistema de lousa eletrônica SHAVI. Cada módulo ficou responsável por uma tarefa nesse ambiente. Com a geração de *logs* de auditoria, é possível analisar o que cada usuário (profissional de saúde) executou no sistema. O controle de acesso ao sistema ficou responsável por quem pode acessar o sistema, permitindo apenas pessoas autorizadas. O nível de acesso também é controlado, isto é, cada usuário consegue acessar apenas sua área de trabalho e visualizar apenas informações que são disponíveis para o seu cargo. Já o *backup* será realizado no final de cada turno do trabalho, em que as informações serão copiadas para um segundo disco localizado em um servidor da Universidade.
Espera-se que os resultados obtidos contribuam com a disponibilidade de informação íntegra e consistente para os usuários do sistema.

Agradecimentos

Agradecemos à equipe de profissionais da saúde do Hospital Universitário de Maringá e à Fundação Araucária pela concessão de bolsas de iniciação científica PIBIC-AF.

Referências

ALMEIDA, J. L., Roecker. N. M., BALANCIERI, R., TEIXEIRA, H. M. P., Dias, M. M., MARTINS, J. S. Sistema de Lousa Eletrônica para Unidade de Urgência e Emergência Médica. In: CBIS 2014 - XIV Congresso Brasileiro de Informática em Saúde, Santos – SP, 2014.
ISO/IEC 27799:2008 - Health informatics — Information security management in health using ISO/IEC 27002. Disponível em: <**http://tc215.behdasht.gov.ir/uploads/244_514_ISO%2027799_2008%20.pdf** >. Acesso em: 03 mar. 2017.
BRASIL. Portaria n° 271, de janeiro de 2017 - Ministério da Saúde. Disponível em: <**http://www.lex.com.br/legis_27287736_PORTARIA_N_271_DE_27_DE_JANEIRO_DE_2017.aspx** >. Acesso em: 03 mar. 2017.