Auditoria em Sistemas de Informação – Trilhas de Auditoria

Cleber dos Santos Garcia, Danilo Dias,
Francisco Braz Mendes Júnior e Juliano de Andrade Almeida

MBA Gestão de Sistemas de Informação – Universidade Católica de Brasília (UCB)
SGAN 916 Avenida W5 – CEP: 70.790-160 – Brasília – DF – Brasil

clebergarcia@uol.com.br, danilod@cabal.com.br,
jr_braz@yahoo.com.br e juliano@sicoobdf.coop.br

Resumo: Existe a necessidade de segurança em sistemas de informação em poder saber quais ações foram executadas e quem as executou. Neste contexto, torna-se necessário um mecanismo de gravação e recuperação das ações ou eventos que foram realizados no sistema. É de grande importância que as informações geradas por este mecanismo sejam precisas, pois formarão as trilhas de auditoria. A geração trilhas de auditoria, a análise e a forma de armazenamento são definidas de acordo com a necessidade da aplicação e são os principais pontos para o planejamento de um sistema de auditoria.

Abstract: *There is the necessity of security in information systems in to be abble knowing wich actions were executed and who executed it. In these context, it become necessary a recording control and recuperation of actions or events that were made in the system. It is important the information created by this recording are right, therefore they will make the audit trace. The generation of audit trace, the analysis and the storage form are defenided in accordance with the necessity of aplication and they are the main points for the planning of an audit system.*

1. Introdução

Um problema comum em segurança é identificar quem ou o que causou algo. Essa identificação é possível pela gravação e manutenção de uma trilha de ações realizadas no sistema, chamadas de trilhas de auditoria. A importância dessa ferramenta será abordada ao longo deste trabalho de forma direta e objetiva, desde seu conceito, geração, análise automática, armazenamento e conformidade com a Common Criteria, conhecida no Brasil como ISO/IEC 15408.

2. O que é Auditoria?

Auditoria em software significa uma parte da aplicação, ou conjunto de funções do sistema, que viabiliza uma auditoria. Isso ocorre pela gravação e manutenção de uma trilha de ações realizadas no sistema e, posteriormente, pela análise ou visualização desta, ou seja, o sistema mantém os registros de tudo o que foi feito nele de forma que, em caso de problema de segurança, alguém possa identificar o que ou quem o causou.

3. Considerações importantes

O processo de auditoria de software pode ser simples de implementar, mas é uma das coisas mais difíceis de se projetar em um sistema. Existem alguns pontos importantes que devem ser analisados antes de se iniciar um processo de auditoria:

- **Que ações devem ser registradas?** Que informações dessas ações devem ser registradas? Registrando tudo, haverá problemas de espaço para tanta informação, lentidão do sistema e acúmulo demasiado de informações. Registrando pouco, corre-se o risco de não identificar justamente aquela ação que permitiria desvendar o problema.
- **O que fazer com a privacidade?** Alguns sistemas exigem requisitos poderosos de privacidade do usuário. A auditoria certamente pode violar a privacidade. Deve-se ignorar a auditoria para preservar a privacidade?
- **Como será feita a análise da trilha?** Normalmente a trilha somente será analisada em caso de problema de segurança. Porém,

muitos problemas de segurança ocorrem sem que se perceba e somente quando os prejuízos forem grandes é que se descobrirá que houve o ataque.

- **Como será armazenada a trilha?** Um arquivo em disco pode ser uma boa opção, mas uma trilha de auditoria que pode ser apagada pelo atacante detectará apenas os ataques mais simples.
- **O que fazer quando não houver espaço para registro na trilha?** Em todos os modos de armazenamento de trilhas de auditoria existe um limite. Em algum momento o espaço acaba. O que fazer? Apagando-se os registros o sistema estará liberado ao ataque. Excluindo-se os registros mais antigos, o *hacker* pode descobrir uma ação lícita que gere muitos registros de auditoria e usá-la seguidamente para apagar sua última ação. Uma outra alternativa é bloquear o sistema, impedindo qualquer ação até que o administrador libere mais espaço, sendo a opção mais segura. Porém, além de prejudicar os usuários do sistema, pode-se sofrer um ataque de negação de serviço (*Denial of Service*) neste sistema.

Como compatibilizar a auditoria com a auditoria do sistema operacional e de outras aplicações? Se todos registrarem os mesmos atos, haverá desperdício de tempo e dinheiro: a mesma ação registrada em vários lugares não tem utilidade, consumindo tempo e espaço. O primeiro ponto que deve ser observado é o objetivo de se utilizar a auditoria. Desconsiderando-se os objetivos externos à segurança do sistema, os objetivos de auditoria podem ser:

- **Segunda linha de proteção:** por que auditar um evento que o sistema de segurança impede que ocorra? Para ser capaz de

responsabilizar o usuário em caso de falha das funções de segurança. Se o ativo é importante, provavelmente já existem mecanismos de segurança lógicos ou de procedimentos que impedem o usuário de atingir este ativo.

- **Melhoria do sistema:** deseja-se medir o funcionamento dos mecanismos de proteção e identificar falhas na proteção, de forma a definir possíveis pontos de melhoria do sistema.
- **Aumento de escopo:** precisa-se identificar seqüências de ações que, embora válidas isoladamente, geram prejuízos ou exposição desnecessária de ativos. Exemplo: é natural que o usuário solicite material de escritório, porém, se ele solicita uma quantidade anormal, pode ser indício de furto.
- **Prevenção:** necessidade de aviso de tentativas de invasão ou ameaças que tentem repetidamente fraudar os mecanismos de segurança do sistema. Neste coso, ocorre um aumento da segurança das funções normais de segurança do sistema.
- **Política:** atendimento à determinação da política de segurança.

4. Geração de dados da Auditoria

Este é o processo mais difícil no projeto de uma auditoria eficiente e eficaz. O registro de um número muito grande de eventos torna a auditoria bastante completa, porém, tornando o sistema lento, aumentando a necessidade de armazenamento e impossibilitando a revisão da trilha de auditoria.

Existem técnicas de abordagem estruturada do problema que permitem uma solução. Como toda solução de compromisso, sempre se corre o risco de

registrar mais ou menos ações do que o necessário, mas a escolha da abordagem correta garante ao menos a coerência.

O principal ponto é definir qual o objetivo do mecanismo de auditoria. Se buscarmos responsabilização e melhoria do sistema de segurança, o *Common Criteria* sugere uma série de eventos para auditoria de cada mecanismo de proteção ou atributo de segurança implementado no sistema.

Para atender aos demais objetivos da auditoria, torna-se necessário sempre fazer a ligação com as ameaças. Uma ameaça à segurança é uma tríade composta por um agente (que tem determinado conhecimento técnico ou poder sobre o sistema), um ativo (informação valiosa para o agente) e um mecanismo (que representa uma vulnerabilidade no sistema). Para se atingir os objetivos de aumento do escopo de proteção e prevenção de ataques, precisa-se auditar levando em consideração os quatro critérios abaixo:

- Principais mecanismos utilizados pelas ameaças ao sistema;
- Ativos mais valiosos;
- Agentes mais capacitados;
- Itens definidos na política de segurança.

Nos demais casos, a base para definição da lista de eventos auditados são ameaças que serão tratadas apenas por meio da auditoria, tanto na forma de aumento do escopo da proteção como de prevenção da ocorrência de ameaça.

Um evento de auditoria será a união de três conjuntos de eventos:

- Eventos exigidos pela política de segurança ou legislação;
- Eventos exigidos pela monitoração da segurança do sistema (responsabilização e melhoria);

- Eventos exigidos pelo tratamento de ameaças via auditoria (aumento de escopo e prevenção)

4.1. Quando gerar dados para a Auditoria

Todo sistema que necessite de um nível mais alto de segurança, principalmente de controle de acesso, precisa também de auditoria. É importante acompanhar o desempenho do sistema de segurança e corrigir eventuais falhas, bem como identificar os usuários maliciosos.

O sistema de auditoria é sempre caro em termos de custo de implantação e perda de desempenho do software.

Um sistema de auditoria tem os seguintes objetivos de segurança:

- Todo usuário deve ser responsabilizado por seus atos;
- O sistema deve ser capaz de permitir a detecção de ataques não previstos na especificação original;
- O sistema deve registrar qualquer alteração na tabela de orçamento;
- O sistema deve permitir a detecção de anormalidades no volume de compras mensais dos responsáveis pelas compras de cada área.

4.2. Conformidade com a ISSO/IEC 15.408

O registro e a visualização da trilha de auditoria são cobertos no *Common Criteria* por três atributos de segurança:

- Geração de dados para auditoria (FAU_GEN);
- Seleção de dados para auditoria (FAU_SEL);
- Revisão de dados da auditoria (FAU_SAR).

A geração de dados de auditoria (FAU_GEN) pode ser implementada isoladamente, mas é aconselhável que seja acompanhada de uma revisão de dados de auditoria (FAU_SAR). Na maioria dos casos, é apropriado incluir também o FAU_SEL (seleção de dados de auditoria), a fim de permitir o aumento do número de eventos da auditoria em caso de suspeita de fraude e a diminuição em períodos de normalidade.

5. Análise automática da trilha de auditoria

Quando o objetivo da auditoria é a detecção de invasões do sistema, a melhoria do sistema ou mesmo a prevenção pela detecção de tentativas de quebra de segurança, é imprescindível que a trilha de auditoria seja periodicamente revista. Nada adiantará registrar todos os eventos se ninguém observar o resultado final para verificar se existe algum ponto fraco ou se ocorreu alguma invasão.

A tarefa de revisar manualmente a trilha de segurança é um pouco frustrante e apresenta altas chances de erro. São milhares de eventos e em 99% das vezes estes não apresentam grandes problemas. Caso o objetivo da auditoria seja apenas o atendimento a questões legais ou a responsabilização em caso de quebra de segurança, é aconselhável um processo simples de revisão e apenas quando ocorrer um fato que gere essa necessidade.

Em qualquer outro caso, é altamente desejável que um mecanismo automático de detecção de problemas seja utilizado. Esse tipo de mecanismo pode ser acionado quando:

- Determinado evento de auditoria, desenhado para proteção por escopo, ocorre em um determinado número de vezes;

- Um grupo de eventos, inofensivo separadamente, mas que, em conjunto, pode indicar tentativa de violação do sistema;
- Determinado evento que indica quebra de controle de acesso do sistema tenha ocorrido.

6. Armazenamento da trilha de auditoria

Um dos problemas mais significativos ao se desenvolver um sistema que registra trilhas de auditoria é o armazenamento dessas trilhas:

- A trilha não pode ser alterada por usuários comuns;
- A trilha precisa estar íntegra, mesmo no caso de ataque ou falha do sistema;
- O que fazer quando não há mais espaço para o armazenamento da trilha de auditoria?
    - Sobrescrever as informações mais antigas?
    - Bloquear o sistema até o administrador liberar mais espaço?
    - Ignorar novos eventos?

No dimensionamento da trilha de auditoria, deve-se sempre trabalhar com valores folgados, a fim de evitar ao máximo de se atingir a situação limite. O administrador deve ser avisado o mais rápido possível da proximidade de exaustão da trilha. Se a exaustão for inevitável, deve-se optar pela alternativa de menor perda para o sistema. Se a confiabilidade é o mais importante, deve-se retirar o sistema do ar até que o administrador libere mais espaço ou descarte a trilha de auditoria. Se a disponibilidade é essencial e o sistema conta com atributos de análise de auditoria e alerta de segurança, pode-se utilizar este

mecanismo para avisar sobre o evento que represente uma violação potencial da segurança.

Outro fator que deve ser estudado é quanto tempo de auditoria será mantido; por exemplo, pode-se definir um procedimento semanal de revisão da trilha e armazenamento manual em mídia (CD/DVD), ou seja, o administrador, uma vez por semana, inspeciona a trilha do sistema em busca de eventuais problemas e, em seguida, armazena essa trilha em mídia. Os discos dos últimos seis meses são armazenados. Esse procedimento deve ser ajustado às necessidades do sistema, mas é importante que exista uma política de descarte dos dados ou de armazenamento em arquivo morto, pois a auditoria gera uma grande quantidade de informações.

Deve-se utilizar o armazenamento de trilha sempre que houver registro de auditoria, observando que alguns sistemas operacionais disponibilizam mecanismos prontos de armazenamento dessa trilha, podendo poupar muito trabalho da equipe de desenvolvimento. O armazenamento da trilha de auditoria é tratado pelo componente FAU_STG do *Common Criteria*.

7. Conclusão

Ter um “rastro” de tudo aquilo que foi feito ou consultado no sistema é um recurso precioso para qualquer administrador. As ações que devem ser registradas, a privacidade do usuário, o modo como será feito a análise e o armazenamento dessa trilha devem ser considerados no planejamento para que não ocorra um desperdício de recursos.

O compartilhamento de recursos e o trabalho em rede, torna a auditoria um processo bastante utilizado e aumenta a sua aplicabilidade nos sistemas em

produção. As trilhas de auditoria possibilitam também, prover um mecanismo de aperfeiçoamento e proteção contra as principais ameaças e vulnerabilidades, na correção de “falhas” diagnosticadas, nas tentativas de acesso e violação do sistema.

Referências

ALBUQUERQUE, Ricardo; RIBEIRO, Bruno. **Segurança no desenvolvimento de software**. Rio de Janeiro: Campus, 2002. 336 p.

DIAS, Cláudia. **Segurança** e **auditoria** da tecnologia da informação. Rio de Janeiro: Axcel Books, 2000. 218 p.

GIL, Antonio de Loureiro. **Fraudes informatizadas**. 2. ed. São Paulo: Atlas, 1999. 202 p.