Curso de Tecnologia em Redes de Computadores
Disciplina: Auditoria e Análise de Segurança da Informação - 4º período
Professor: José Maurício S. Pinheiro

AULA 4: Trilhas de Auditoria

Existe a necessidade de segurança em sistemas de informação para 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.

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

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.

Auditoria

Negócios são suportados por processos que mantêm uma relação de dependência de ativos físicos, tecnológicos e humanos, que possuem falhas de segurança. Estas por sua vez, são potencialmente exploradas por ameaças que, se são bem-sucedidas na investida, geram impactos nos ativos, estendendo-os aos processos até que, finalmente, atingem os negócios. Possuir uma visão integrada dos riscos é fundamental para as empresas que buscam o desenvolvimento e a continuidade do negócio, e ainda dependem de uma infra-estrutura operacional sob risco controlado (Figura 1). 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.

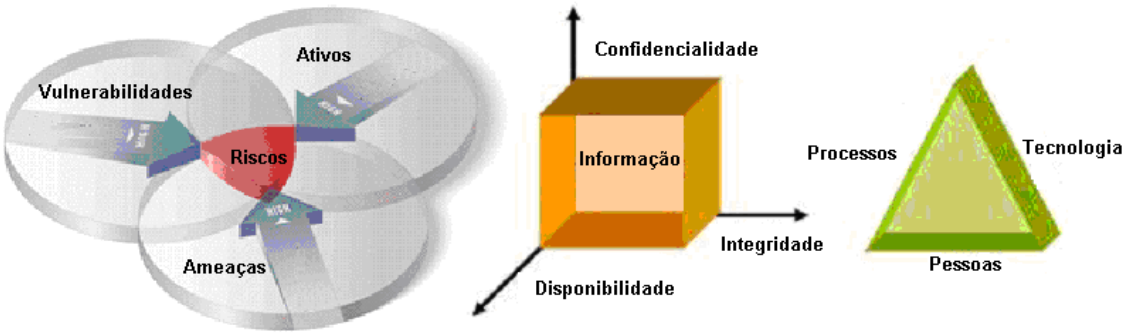

Figura 1 - Análise de riscos no negócio

Auditoria em SI 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.

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. Assim, o processo de auditoria apresenta alguns pontos importantes que devem ser analisados antes de se iniciar um processo de auditoria propriamente dito:

- **Ações** - quais ações devem ser registradas e quais informações dessas ações devem ser registradas? Registrando tudo, haverá problemas de espaço para o volume de 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;
- **Privacidade** - Alguns sistemas exigem requisitos de privacidade do usuário. A auditoria pode violar a privacidade. Deve-se ignorar a auditoria para preservar a privacidade?
- **Análise da trilha** - Normalmente a trilha somente será analisada em caso de problema de segurança;
- **Armazenamento** - 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. Em todos os modos de armazenamento de trilhas de auditoria existe um limite. Em algum momento o espaço acaba. 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 alternativa é bloquear o sistema, impedindo qualquer ação até que o administrador libere mais espaço, sendo a opção mais segura.

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** - 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 as falhas na proteção, de forma a definir possíveis pontos de melhoria do sistema.
- **Aumento de escopo** - identificar seqüências de ações que, embora válidas isoladamente, geram prejuízos ou exposição desnecessária de ativos.
- **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 e aplicação à determinação da política de segurança.

O segundo ponto que deve ser observado é que um sistema de auditoria é sempre caro em termos de custo de implantação e perda de desempenho do software. Um sistema de auditoria deve apresentar 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 nos registros de dados;
- O sistema deve permitir a detecção de anormalidades no volume de dados manipulados pelos usuários a fim de detectar uso anormal e ou abusivo.

Geração de dados da Auditoria

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. 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 análise das ameaças.

Para se atingir os objetivos de aumento do escopo de proteção e prevenção de ataques, a auditoria é necessária levando em consideração quatro critérios:

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

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 uma vez que a trilha não pode ser alterada por usuários comuns e necessita estar íntegra, mesmo no caso de ataque ou falha do sistema.

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 considerado é quanto tempo de auditoria será mantido. Pode-se definir um procedimento semanal de revisão da trilha e armazenamento manual (CD, DVD, DAT, etc.), ou seja, o administrador, uma vez por semana, inspeciona a trilha do sistema em busca de eventuais problemas e, em seguida, armazena na mídia selecionada. 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.

Evento de Auditoria

A base para definição da lista de eventos auditados inclui as 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 (responsabilização e melhoria);
- Eventos exigidos pelo tratamento de ameaças através da auditoria (aumento de escopo e prevenção).

Conformidade com a ISO/IEC 15.408

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. 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.

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

- Geração de dados para auditoria;
- Seleção de dados para auditoria;
- Revisão de dados da auditoria.

A geração de dados de auditoria pode ser feita isoladamente, mas é aconselhável que seja acompanhada de uma revisão de dados de auditoria. Na maioria dos casos é apropriado incluir também a 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.

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.

Processo de Auditoria

A auditoria tem como verificar se os requisitos para segurança da informação estão implementados satisfatoriamente, mantendo a segurança nos dados da empresa e verificando se os seus bens estão sendo protegidos adequadamente. Assim, segurança e auditoria são interdependentes, ou seja, uma depende da outra para produzirem os efeitos desejáveis na administração do negócio. Enquanto a segurança tem a função de garantir a integridade dos dados, a auditoria vem garantir que estes dados estejam realmente íntegros propiciando um perfeito processamento, obtendo os resultados esperados.

A auditoria é de vital importância para empresa, já que através desta os administradores ditam os rumos do negócio, além de evitar fraudes e garantir o bom desempenho dos setores auditados. O processo de auditoria é composto por: Pré-Auditoria, Auditoria e Pós-Auditoria.

- **Pré-Auditoria** - o auditor deve preparar as atividades administrativas necessárias para a realização da auditoria, definir as áreas a auditar, orientar o grupo de auditores quanto à estratégia a ser adotada, preparar o documento de anúncio e anunciar o setor da Auditoria;
- **Auditoria** - o auditor deve avaliar os controles (como a área auditada funciona); documentar os desvios encontrados (falhas); validar as soluções, preparar o relatório final e apresentá-lo para os responsáveis legais. O setor auditado deve prover as informações necessárias ao trabalho da auditoria, analisar a exposição dos desvios encontrados, entender os desvios encontrados, desenvolver planos de ação que solucionarão os desvios encontrados;
- **Pós-Auditoria** - o setor auditado deve solucionar os desvios encontrados pela auditoria, preparar um relatório, administrar conclusão dos desvios e manter o controle para que os erros não se repitam e a eficácia seja mantida. O auditor deve distribuir o Relatório Final, revisar resposta recebida (soluções e justificativas apresentadas), assegurar o cumprimento e analisar a tendência de correção.

O Papel do Auditor

O auditor deve revisar o plano aprovado na política de segurança, ou seja, verificar se o método utilizado para proteção de informações é adequado ou se necessita de alguma atualização, sempre relacionado com o esquema de trabalho da área que está sendo auditada.

Depois de terminado o estudo do plano, o auditor deve solicitar os procedimentos que descrevem as diversas atividades que necessitam de segurança. Esses procedimentos são confrontados com a realidade do dia-a-dia, ou seja, é verificado se todos os procedimentos necessários à segurança são corretamente utilizados.

Na investigação o Auditor deverá revisar os seguintes itens:

- O proprietário da informação (aquele que tem permissão para acessar certo conjunto de informações), periodicamente faz uma revisão em todos os dados que ele tem acesso para verificar se houve perdas, alterações, ou outros

eventos de qualquer natureza. A administração da rede deve ser notificada sobre os resultados da revisão tanto quando eles forem favoráveis (os dados estão corretos) ou quando for encontrada alguma irregularidade;

- Todos os proprietários estão identificados, ou seja, os que possuem acesso a um conjunto de informações específicas;
- Os inventários são realizados periodicamente conforme requerido e padronizado pela política de segurança;
- Os dados possuem a proteção necessária para garantir sua integridade, disponibilidade e confidencialidade;
- A documentação dos processos é avaliada pelas áreas competentes, garantindo que estas demonstrem o que realmente ocorre dentro da área a que se está referindo a documentação;
- Quando ocorrem desastres, desde um erro de digitação até a perda total dos dados de um banco de dados, existem planos de recuperação que são testados periodicamente;
- Os programas críticos estão seguros o suficiente de modo que qualquer tentativa de fraude não consiga alterar o conteúdo dos dados no sistema;
- Um terminal oferece acesso somente às informações inerentes a ele por meio de uma política de senhas, estando protegido assim, contra acessos não autorizados;
- O processo de auto-avaliação da área auditada foi feito e concluído com sucesso;
- Somente os usuários autorizados têm acesso aos sistemas. Pessoas não autorizadas não poderão manipular, obter ou influenciar os dados do sistema.