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

AULA 8: Auditoria da Segurança

Quando se pensa em segurança de informação a primeira idéia que surge é a proteção da mesma, não importando onde esteja armazenada. Mas a segurança da informação vai além. Deve satisfazer também a expectativa dos usuários no aspecto de que esta esteja disponível no local e no momento que necessitar que o conteúdo seja confiável, os dados corretos e que esteja protegida dos acessos não autorizados.

1. Incidentes de Segurança

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

São exemplos de incidentes de segurança:

- Tentativas de acessos não autorizados aos sistemas ou dados;
- Ataques de negação de serviço;
- Uso ou acesso não autorizado a um sistema;
- Modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do proprietário do sistema;
- Desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

O problema é que mesmo tomando-se todas as medidas necessárias, falhas de segurança podem ocorrer, uma vez que alguma vulnerabilidade ainda não divulgada pode ser explorada ou um novo tipo de ataque pode ser utilizado. Dessa forma, não há como afirmar que um dado sistema de segurança está isento de falhas. Isto se deve principalmente ao fato de que tais sistemas, bem como os serviços oferecidos na rede, são compostos por diversos softwares, que por sua vez, possuem milhares de linhas de código que não estão imunes a erros de programação.

Existem atualmente mais de 4.500 formas conhecidas de ataques através da Internet. Os ataques conhecidos são baseados em vulnerabilidades típicas das aplicações web e tem se concentrado nas portas publicas (80 e 443) que não devem ser bloqueadas pelos firewalls comuns, pois os visitantes não acessariam os sites, nem as aplicações. Mesmo os firewalls mais modernos não conseguem analisar e filtrar a camada de Aplicação (camada 7 do modelo OSI).

Uma aplicação típica, geralmente, está distribuída em vários servidores, rodando diversos aplicativos e para funcionar na velocidade adequada, ela necessita que as interfaces entre os diversos sistemas sejam construídas com a premissa que os dados passados através da mesma são confiáveis e não hostis. Não há tempo hábil para duplas verificações. O ponto fraco destas aplicações é a necessidade de haver “confiança” entre os diversos subsistemas e é disso que os hackers e outros criminosos se aproveitam.

Os ataques podem causar uma série de problemas, entre os quais:

- Perdas Financeiras;
- Transações Fraudulentas;
- Acesso não autorizado aos dados, inclusive informações confidenciais;
- Roubo ou modificação de Dados;
- Roubo de Informações de Clientes;
- Interrupção do Serviço;
- Perda da confiança e lealdade dos clientes;
- Dano à imagem da marca.

A segurança dos produtos disponíveis no mercado é assegurada pelos fabricantes, que fornecem periodicamente correções que os atualizam. Para o sistema aplicativo, freqüentemente desenvolvido localmente ou por terceiros, especificamente para a empresa, não existem correções de segurança. Segundo recentes pesquisas, aproximadamente 75% dos ataques ocorrem sobre os aplicativos específicos de cada empresa.

Tendo em vista que não há esquema de segurança imune a falhas, torna-se então necessária a definição de procedimentos a serem adotados no caso de um ataque bem sucedido, além da presença de pessoal capaz de executar tal função.

No caso da ocorrência de um incidente de segurança, é vital, mas ainda raro, o estabelecimento de programas de resposta a incidentes, nos quais estão incluídas as metodologias de análise e uma política de uso aceitável da rede. A política de uso aceitável da rede é um documento que define como os recursos computacionais da organização podem ser utilizados. Também é ela quem define os direitos e responsabilidades dos usuários. As empresas costumam dar conhecimento da política de uso aceitável no momento da contratação ou quando o funcionário começa a utilizar os recursos computacionais.

2. Tipos de usuários

Existem basicamente dois tipos de usuários em redes de computadores, ambos com características perfeitamente definidas: usuários operacionais (ou de processamento) e usuários fonte.

O que se torna necessário é definir quais as operações que estarão disponíveis para cada um deles, e compreender perfeitamente bem como uma Política de Segurança da Informação alcançará o sucesso desejado, a partir da adoção de medidas restritivas de acessibilidade aos dados.

2.1. Usuários Operacionais ou de Processamento

São definidos como aqueles que necessitam utilizar os dados para qualquer tipo de processamento. As operações de processamento são baseadas em ações não degenerativas. Logicamente, restringindo a acessibilidade a tais operações, não se corre o risco de alterações dos valores iniciais dos dados. Resta definir o nível de acesso de cada um desses usuários (de acordo com as restrições de acessos) para se ter certeza de que o objetivo de preservar os dados estará sendo alcançada.

2.2. Usuários Fonte

Usuários fonte são aqueles que originam os dados, aquele que gera o dado. Esses usuários devem ser criteriosamente escolhidos, pois são de fundamental importância para a empresa. A eles e somente a eles devem ser fornecidas acessibilidades para que realizem operações de manipulação de dados que se baseiam em ações degenerativas.

Um Usuário Fonte pode vir a ser também um Usuário Operacional, todavia para estes casos devem ser bem separadas e analisadas essas duplicidades funcionais para que não firam os conceitos acima determinados.

3. Restrições de acesso aos dados

A garantia da integridade dos dados prevê, ainda, outras ações que permitirão a criação de rotinas gerais de administração dos mesmos. Assim a cada acesso a um dado ou grupo de dados devem-se seguir os seguintes passos:

- **Identificar o Usuário** - o usuário deve ser identificado, através de uma senha e uma identificação de acesso (*login*) que determina a sua acessibilidade e qual o seu nível de acesso dos dados;
- **Validar o Usuário** - a partir da validação da senha e do *login*, o usuário deve ser transportado para a sua área de acesso, onde passará a ter os dados disponibilizados com total controle;
- **Conceder Privilégios** - dependendo do nível em que se encontram, os usuários poderão receber privilégios, desde que não venham a ferir os níveis de acessibilidades e segurança.

O fato de um usuário ter sido identificado e autenticado não quer dizer que ele poderá acessar qualquer informação ou aplicativo sem qualquer restrição. Deve-se formalizar um controle específico, restringindo o acesso dos usuários apenas às aplicações, arquivos e utilitários imprescindíveis para desempenhar suas funções na organização. Esse controle pode ser feito por menus, funções ou arquivos.

A concessão de privilégios e acessibilidades pode levar em consideração aspectos funcionais dentro da empresa, assim os privilégios passarão a gerar senhas por grupos funcionais que identificarão as funções departamentais de cada um dos usuários, além da identificação pessoal do mesmo. A garantia do nível de acessibilidades também estará sendo obtida, pois esta senha grupal deverá adotar o que chamamos de senhas por herança hierárquica em diversos níveis. Essas senhas por herança podem ainda conter o que denominamos de heranças múltiplas funcionais, ou seja, um mesmo usuário tem acessibilidades a grupos de dados cuja origem tem outras funções diferentes da sua.

4. Segurança em Banco de Dados

A segurança das informações, como um todo, depende do esquema de segurança do Banco de Dados (BD) onde as mesmas estão armazenadas. Quando esta segurança é quebrada, seja acidentalmente, ou propositadamente, os resultados são altamente prejudiciais. Por esse motivo, a segurança dos BD é uma questão muito importante quando se desenvolve o projeto de política de segurança computacional.

A segurança dos dados visa proteger a integridade dos mesmos, ou seja, garantir que eles somente sejam alterados, ou excluídos por pessoas autorizadas a efetuar tais operações (usuários fonte). Todavia, a segurança e a integridade dos dados não dependem somente das autorizações concedidas a essas pessoas, mas sim, da maneira como se controla o acesso dessas pessoas, uma vez que elas podem, perfeitamente, “contrabandear” os dados que elas controlam. Pode-se citar como exemplo, a espionagem industrial, como sendo uma forma de contrabando de dados, de maneira voluntária e executada por pessoas que têm acesso garantido aos referidos dados e praticam livremente essa ação.

Enquanto a permissão de acesso define o que um usuário pode ou não fazer no sistema, uma lista de controle de acesso define o que os outros usuários podem fazer com os sistemas a eles associado. As listas de controle de acesso nada mais são do que bases de dados, associadas a um objeto, neste caso, um usuário, que descrevem os relacionamentos entre aquele objeto e outros, constituindo-se em um mecanismo de garantia de confidencialidade e integridade de dados. A definição das listas de controle de acesso deve ser sempre feita pelos proprietários dos recursos, os quais determinam o tipo de proteção adequada a cada recurso e quem efetivamente terá acesso a eles.

4.1. Implementação da Segurança em Banco de Dados

O primeiro passo para a implementação de segurança de Banco de Dados requer a garantia do estabelecimento de uma política de privacidade e segurança, isso é, a definição do ambiente computacional que irá armazenar os dados, bem como a definição de controles físicos, humanos e procedimentais do acesso aos dados. Essa política irá definir o que deve ser feito e não como fazê-lo.

O passo seguinte é mostrar os mecanismos que serão utilizados para cumprir as funções pretendidas pela política de segurança de dados. O último passo a ser implementado é a garantia de que os mecanismos adotados cumpram, com alto grau de confiabilidade, a política de segurança. Quanto mais alta for essa garantia, mais difícil será quebrar a política de segurança.

As políticas de seguranças de Bancos de Dados devem levar em consideração três objetivos fundamentais:

- **Segredo** – Prevenir o acesso às informações por usuários não autorizados, como por exemplo: em um sistema de folha de pagamento, um empregado de nível inferior não deve ter acesso aos salários de seus superiores.
- **Integridade** – Evitar modificações das informações por usuários não autorizados a executar esse procedimento, como por exemplo: neste mesmo sistema de folha de pagamento evitar que um usuário altere o seu salário, sem que para isso esteja autorizado.
- **Disponibilidade** – Prevenir que algum fator impeça os acessos aos dados e às informações, como por exemplo, no sistema de folha de pagamento os contracheques deverão ser impressos e entregues no prazo previsto.

4.2. Sistema Gerenciador de Banco de Dados

As empresas modernas não podem arriscar seus dados e informações, deixando que eles estejam desprotegidos pela adoção de um SGBD que não ofereça os requisitos necessários aos níveis de segurança desejados. O problema de segurança envolve aspectos tanto políticos quanto técnicos.

A escolha correta de um Sistema Gerenciador de Banco de Dados tem, obrigatoriamente, que passar por uma análise criteriosa não só com relação aos aspectos operacionais que este gerenciador oferece, mas também em relação às características de segurança que ele possibilita. Não é uma tarefa simples, todavia, da adoção de critérios rígidos e bem formulados é que resultará em níveis de segurança maiores ou menores.

A maioria dos Sistemas Gerenciadores de Bancos de Dados compartilha a garantia da segurança com os Sistemas Operacionais, fazendo com este aspecto passe a ser um assunto tratado de forma integrada entre esses dois níveis e gerenciado pela integração desses dois sistemas. Obviamente, em caso de má integração ou mesmo de falha na observação dos aspectos de segurança de qualquer um dos dois sistemas, poderá ocasionar “brechas” e falhas que somente serão percebidas por uma análise criteriosa por parte dos auditores de segurança.

5. Custo da Segurança na Web

Uma aplicação web típica apresenta entre 150 mil a 250 mil linhas de código. Lidam com vários subsistemas, bancos de dados e sistemas operacionais. Na sua especificação são observados normalmente quesitos como rapidez de processamento (os visitantes não gostam de esperar), beleza e usabilidade (a idéia é transformar visitantes em clientes), prazo de entrega e custo baixo.

Normalmente segurança não faz parte dos requisitos do sistema e quanto existe, não se prevê nenhum mecanismo periódico de atualização em função de novas ameaças. Normalmente, a segurança é subentendida como um problema do pessoal da segurança, da infraestrutura e não do pessoal de desenvolvimento ou produto, a não ser em termos de generalidades.

Softwares que analisam aplicações são de grande ajuda para garantir a qualidade em termos de segurança. O que esses softwares não fazem é corrigir a parte defeituosa identificada no código. Isto deve ser feito por analistas e programadores que conheçam o sistema, tenham sido treinados em segurança e sigam uma metodologia que garanta o desenvolvimento de aplicações seguras.

Considerando os estudos na área, cada 1.000 linhas de código embutem 15 defeitos de segurança. Considerando uma aplicação de 200 mil linhas, existirão, portanto, 3.000 defeitos de segurança, que precisarão ser identificados e corrigidos. Um estudo de cinco anos, realizado pelo Pentágono, nos Estados Unidos, estima que se gastem 75 minutos em media para identificar um defeito de segurança e de 2 a 9 horas para corrigi-lo. Pode-se estimar facilmente o numero de horas necessárias para se corrigir todos os defeitos de segurança de uma aplicação típica, supondo-se 5 horas de analista/programador para identificar e corrigir um defeito de segurança:

200.000 linhas / 1.000 linhas por defeito x 15 defeitos x 5 horas = 15.000 horas

Cada aplicação demandaria 15 mil homens / hora de analista / programador para ser corrigida. Supondo que cada analista / programador trabalhe 6 horas por dia, vezes 22 dias úteis, são 132 horas de trabalho por mês, ou seja, a aplicação demandaria 114 homens / mês, e se fossem alocados 4 pessoas na equipe de correção, o sistema estaria pronto e corrigido em 29 meses.

Alem do tempo necessário para corrigir os erros e defeitos, o custo, muitas vezes escondido na forma de custos fixos, passa a ser um desafio importante. Tudo isso supondo que a aplicação não sofra melhorias e manutenções, que certamente introduzirão novas falhas de segurança.

5.1. Serviços Web

Os Serviços Web seguem a Arquitetura Orientada a Serviços (SOA) e as principais características que os tornam uma tecnologia integradora e promissora são:

- Possuem um modelo fracamente acoplado e transparente que garante a interoperabilidade entre os serviços, sem que estes necessitem ter o conhecimento prévio de quais tecnologias estão presentes em cada lado da comunicação;
- Usam padrões abertos como o HTTP e XML, por exemplo, permitindo que aplicações sejam integradas através de linguagens e protocolos amplamente aceitos;
- Facilitam a composição ou a combinação de diferentes provedores, visando formar serviços mais complexos.

Os Serviços Web estão suscetíveis a alguns tipos de ataques já conhecidos como negação de serviço (DoS), mensagens antigas, estouro de pilha, entre outros. Para garantir a segurança neste tipo de ambiente, novos mecanismos de segurança devem ser implantados também nas camadas superiores da pilha TCP/IP e devem operar em conjunto com os mecanismos presentes nas camadas inferiores (Figura 1).

Figura 1 - Segurança nas diversas camadas

Além das propriedades básicas de segurança, a concepção de aplicações baseadas nos Serviços Web deve considerar pontos como a transposição de domínios administrativos e de segurança, o que acarreta em preocupações com a privacidade, o anonimato, a evolução das políticas de segurança, e principalmente, a interoperabilidade.

Com o objetivo de tornar seguro o uso dos Serviços Web, muitas propostas estão sendo analisadas visando cobrir diversas áreas de segurança e, em conjunto com as especificações de segurança para o padrão XML, estas propostas permitirão garantir alguns dos requisitos de segurança necessários para as aplicações.

5.2. Obtendo Segurança nas Aplicações

Para obter segurança nas aplicações para Internet ou Intranet, é preciso cuidar de quatro elementos básicos: segurança na estação (cliente), segurança no meio de transporte, segurança no servidor, segurança na Rede Interna.

5.2.1. Segurança na Estação

Nas aplicações Web, um dos elementos mais vulneráveis é a estação de trabalho, onde normalmente é executado um acesso via browser ou uma aplicação dedicada por onde o usuário tem acesso aos recursos e serviços da rede.

Estações de trabalho estão ainda sujeitas a execução de programas desconhecidos (como Applets Java, ActiveX e Javascripts) sendo expostas a grampos e outras armadilhas para obtenção de acesso ilícito.

5.2.2. Segurança no Meio de Transporte

Para garantir a privacidade e integridade das informações enviadas pela web, é necessário implementar a segurança no meio de transporte.

5.2.3. Segurança nos Servidores

O uso da web exige segurança nos servidores. As empresas têm conectado sua rede interna à Internet, mas não gostariam de conectar a Internet à rede interna. Para isto, torna-se necessário o uso de firewalls que protegem o acesso através de um servidor de controle no ponto único de entrada/saída dos dados.

5.2.4. Segurança na Rede Interna

O desconhecimento técnico da segurança, a ausência do foco e disciplina no assunto, além da ausência da adoção de uma política de segurança consistente serão os principais fatores para o aumento dos riscos na web.

A segurança deve prever a proteção e controle da rede interna. O modelo para segurança deve assumir riscos internos e externos, ou seja, os desenvolvedores de sistemas e administradores de rede devem utilizar uma estratégia de controle de acesso externo e interno para os usuários.

6. Monitoramento dos Sistemas de Informação

O monitoramento dos sistemas de informação é feito, normalmente, pelos registros de *log*, trilhas de auditoria ou outros mecanismos capazes de detectar invasões. Esse monitoramento é essencial à equipe de segurança da informação, uma vez que é praticamente impossível eliminar por completo todos os riscos de invasão por meio da identificação e autenticação de usuários.

Na ocorrência de uma invasão, falha do sistema ou atividade não autorizada, é imprescindível reunir evidências suficientes para que possam ser tomadas medidas corretivas necessárias ao restabelecimento do sistema às suas condições normais, assim como medidas administrativas e/ou judiciais para investigar e punir os invasores.

A forma mais simples de monitoramento é a coleta de informações, sobre determinados eventos, em arquivos históricos, mais conhecidos como *logs*. Com essas informações, a equipe de segurança é capaz de registrar eventos e de detectar tentativas de acesso e atividades não autorizadas após sua ocorrência. Os *logs* são registros cronológicos de atividades do sistema que possibilitam a reconstrução, revisão e análise dos ambientes e das atividades relativas a uma operação, procedimento ou evento, que serão acompanhados desde o início até o fim.

Os logs são utilizados como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de *logon* ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando. Com os dados dos *logs*, pode-se identificar e corrigir falhas da estratégia de segurança. Por conterem informações essenciais para a detecção de acesso não autorizado, os arquivos de *log* devem ser

protegidos contra alteração ou destruição por usuários ou invasores que queiram encobrir suas atividades.

Devido à grande quantidade de dados armazenada em *logs*, deve-se levar em consideração que seu uso pode degradar o desempenho dos sistemas. Sendo assim, é aconselhável balancear a necessidade de registro de atividades críticas e os custos, em termos de desempenho global dos sistemas.

Normalmente, os registros de *log* incluem:

- Identificação dos usuários;
- Datas e horários de entrada (*logon*) e saída do sistema (*logoff*);
- Quando possível, sua localização;
- Registros das tentativas de acesso (aceitas e rejeitadas) ao sistema;
- Registros das tentativas de acesso (aceitas e rejeitadas) a outros recursos.

Ao definir o que será registrado, é preciso considerar que grandes quantidades de registros podem ser inviáveis de serem monitoradas. Nada adianta ter um *log* se ele não é periodicamente revisado. Para auxiliar a gerência de segurança na tarefa de análise de *logs*, podem ser definidas trilhas de auditoria mais simples e utilizados *softwares* especializados disponíveis no mercado, específicos para cada sistema operacional.