

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

AULA 5: Avaliação de Padrões de Segurança de Computadores

A tecnologia da informação é um componente vital e cada vez maior da vida moderna. No entanto, a mesma tecnologia que permite que as pessoas acessem, gerenciem e compartilhem informações instantaneamente pode ser usada de forma indevida por indivíduos e empresas para invadir a privacidade alheia.

A avaliação de padrões de segurança de computadores define vários níveis de segurança. Estes níveis descrevem diferentes tipos de segurança física, autenticação de usuário, confiabilidade do sistema operacional, e aplicações de usuário. Estes padrões de segurança também impõem limites em que tipos de outros sistemas podem ser conectados a um sistema de computador específico. A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

1. Controles de Acesso

Os controles de acesso, físicos ou lógicos, têm como objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. Os sistemas computacionais, bem diferentes de outros tipos de recursos, não podem ser facilmente controlados apenas com dispositivos físicos, como cadeados, alarmes ou guardas de segurança.

A proteção aos recursos computacionais baseia-se nas necessidades de acesso de cada usuário, enquanto que a identificação e autenticação do usuário (confirmação de que o usuário realmente é quem ele diz ser) são feitas normalmente por meio de um identificador de usuário (ID) e por uma senha durante o processo de entrada (*logon*) no sistema.

Entretanto, 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 utilizar 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.

2. Níveis de Segurança

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

Os Sistemas Operacionais estão classificados, segundo o nível de segurança, em quatro categorias: A, B, C, D, ordenados de maneira hierárquica crescente, com a maior divisão (A) reservada aos Sistemas que oferecem maior nível de segurança. Nas divisões C e B existem subdivisões conhecidas como classes as quais também estão ordenadas hierarquicamente.

2.1. Nível A (Desempenho Verificado)

Trata-se do nível mais alto especificado nos padrões de segurança das redes de computadores. Este nível inclui um projeto e controle rígidos e um processo de verificação. É atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança total dos sistemas, não apresentando falhas de segurança.

Os Sistemas da classe A são funcionalmente equivalentes aos sistemas da classe B3, na medida em que não são acrescentadas características novas em sua arquitetura, ou exigências de planos de ações. A característica que distingue os sistemas desta classe é a análise derivada da especificação formal do desempenho, o emprego de técnicas de verificação e o alto nível de segurança resultante da forma correta com que a Política de Segurança é estruturada.

Esta segurança é progressiva por natureza, começando com um modelo formal do projeto de segurança e uma especificação formal de alto nível do desempenho. De acordo com o seu desempenho ostensivo e da análise do custo da segurança exigida para os sistemas da classe A, requer-se um gerenciamento mais rígido da validação dos usuários e os procedimentos de segurança são estabelecidos para a distribuição segura dos sistemas para os sites.

Para alcançar o nível A de segurança, devem ser incluídos todos os componentes dos mais baixos níveis de segurança, o projeto deve ser verificado matematicamente, e uma análise de canais cobertos e distribuição confiável devem ser executadas. Distribuição confiável significa que o hardware e software são protegidos de modificações durante o seu transporte.

2.2. Nível B1 (Proteção de Segurança Criptografada)

O Nível B1 suporta segurança de múltiplos níveis, estabelecendo que um objeto sob controle de acesso obrigatório não pode ter suas permissões mudadas pelo proprietário do objeto. Este nível é atribuído aos sistemas operacionais que também possuem ferramentas ou capacidades de garantir a segurança em um nível médio, todavia o aspecto que o diferencia do nível C2 é a sua capacidade de armazenamento de todos os "logins" de acesso ao sistema por um tempo mínimo de 2 anos.

Os Sistemas de nível B1 devem possuir todas as características exigidas para os Sistemas de nível C2, além do que, devem estar presentes: uma exposição informal do modelo do projeto de segurança; a classificação dos dados; e o controle obrigatório do acesso aos usuários e aos objetos nomeados. Deve ainda existir uma capacidade de exportar informações de forma criptografada.

2.3. Nível B2 (Proteção Estruturada)

O Nível B2 requer que todo objeto no sistema seja rotulado. Dispositivos tais como unidades de disco e terminais devem ter um único ou múltiplo nível de segurança atribuído a eles. Este nível é atribuído aos sistemas operacionais que também possuem ferramentas ou capacidades de garantir a segurança em um nível médio, todavia o aspecto que o diferencia do nível B1 é a sua capacidade de armazenamento de todos os "logins" de acesso ao sistema por um tempo mínimo de 7 anos.

Nos Sistemas de nível B2 o cálculo do custo da segurança se baseia em um modelo de projeto de segurança formal, claramente definido e documentado, exigindo

que o esforço no controle do acesso discricionário e obrigatório encontrado nos sistemas da classe B1, seja estendido a todos os usuários e objetos de dados.

2.4. Nível B3 (Domínios de Segurança)

O Nível B3 assegura o domínio com a instalação de hardware. Por exemplo, hardware de administração de memória é usado para proteger o acesso sem autorização ao domínio de segurança ou modificação de objetos em domínios de segurança diferentes. Este nível também requer que o terminal do usuário se conecte ao sistema através de um caminho confiável.

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança em um nível bastante alto. O custo do projeto de segurança no nível B3 deve satisfazer as exigências do sistema monitor de segurança, de forma que ele possa medir todos os acessos de usuários aos objetos de dados, além disso, ser razoavelmente imune às invasões e suficientemente pequeno para que possa ser submetido a análises e testes.

2.5. Nível C1 (Proteção Arbitrária)

O Nível C1 também é conhecido como *Discretionary Security Protection System*. Descreve a segurança disponível na maioria dos sistemas corporativos. Neste nível temos uma proteção básica para o hardware. Os usuários têm que se identificar no sistema por um nome de *login* de usuário e uma senha. Este mecanismo de autenticação é usado para determinar os direitos de acesso e as permissões (de arquivo e permissões de diretório) para os usuários.

Estes controles de acesso permitem ao administrador de sistema ou o proprietário de um arquivo ou diretório impedir que certos indivíduos ou grupos tenham acesso a informações ou programas. No Nível C1 muitas tarefas de administração de sistema somente podem ser realizadas por um usuário com poderes de administrador do sistema.

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidade de garantir a segurança sob aspectos mínimos, sem grandes valores de segurança. O custo do projeto de segurança deste nível satisfaz as exigências de segurança discricionária, separando os usuários dos dados. Ele incorpora alguns tipos de controle, capazes de reforçar as limitações de acesso numa base de dados individual. Isto é, ele foi criado de forma que, ostensivamente, permita aos usuários a capacidade de proteger o projeto ou as informações privadas e impedir que outros usuários tenham uma leitura acidental, ou a destruição dos seus dados. O ambiente de classe C1 deve ser o de usuários cooperando entre si e processando dados no mesmo nível.

2.6. Nível C2 (Proteção de Acesso Controlado)

Além das características especificadas para o Nível de segurança C1, o Nível C2 soma características de segurança que criam um ambiente de acesso controlado. Este ambiente tem a capacidade para restringir a execução de certos comandos pelos usuários ou ainda o acesso a arquivos específicos baseado em permissões e níveis de segurança.

O Nível C2 especifica também que o sistema pode ser auditado. Isto envolve a criação de um registro de auditoria para cada evento de sistema. A auditoria requer autenticação adicional para assegurar que a pessoa que executa o comando é de fato a pessoa representada pelo *login*.

Por causa das autorizações adicionais requeridas por C2, é possível para os usuários terem a autoridade para executar tarefas de administração de sistema sem o perfil de administrador do sistema ou usuário *root*. Isto facilita e melhora a identificação de quem executou as tarefas de administração.

Este nível é atribuído aos sistemas operacionais que possuem ferramentas ou capacidades de garantir a segurança em um nível médio, com alguns aspectos complementares de segurança, onde o arquivo de senhas é oculto aos usuários e utilizam um método forte de criptografia de dados. Os Sistemas desta classe reforçam o controle de acesso discricionário, de forma mais precisa do que os sistemas da classe C1, tornando os usuários responsáveis individualmente por suas ações através de procedimentos de “logins”, incluindo a capacidade de realizar auditoria de segurança em eventos.

2.7. Nível D

O Nível D é o mais baixo nível de segurança disponível. Aplica-se aos sistemas operacionais que não distinguem um usuário de outro e não tem nenhum método definido de determinar quem está usando o sistema. Este tipo de sistema é muito encontrado em ambientes e plataformas monousuário.

Os sistemas não apresentam nenhum mecanismo de controle para especificar que informação pode ser acessada dos discos rígidos. Neste nível temos:

- Sistema Operacional não é confiável;
- Nenhuma proteção está disponível para o hardware;
- Aplicações são facilmente comprometidas;
- Os usuários não são autenticados;
- Não há restrição nos direitos para acesso a informações armazenadas no computador.

3. Gestão de Riscos

Negócios são suportados por processos que mantêm uma relação de dependência de ativos físicos, tecnológicos e humanos, que possuem falhas de segurança e, conseqüentemente, riscos. O risco é definido como a expectativa de perda expressiva ou a probabilidade de uma ameaça explorar uma falha de segurança, causando algum resultado prejudicial.

AS falhas de segurança por sua vez, são potencialmente exploradas por ameaças que, se são bem-sucedidas na investida, geram impactos de primeiro nível 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 que ainda dependem de uma infraestrutura operacional sob risco controlado (Figura 1).



Figura 1 - Ciclo de Segurança da Informação

O comportamento das pessoas diante de medidas e contramedidas de segurança faz toda a diferença. A perenidade dos seres humanos é certa e, apesar de um cenário onde a tecnologia está cada vez mais presente, o ser humano sempre estará por trás das decisões, das tecnologias e dos controles dos sistemas. Desta forma, não é inteligente montar uma estratégia de segurança exclusivamente baseada na tecnologia, mas uma solução que considere como peça chave o elemento humano atuante sobre esta tecnologia.

***O que não se conhece não se pode controlar.
O que não se controla não se pode mensurar.
O que não se mensura não se pode gerenciar.
O que não se gerencia não se pode aprimorar.***

3.1. Métodos de Avaliação de Riscos

A maturidade na gestão de riscos é alcançada quando ela não for perceptível. Quando os processos estiverem bem definidos e documentados, orientando os agentes humanos e prontos para suportar mudanças corriqueiras nos ativos físicos, tecnológicos e humanos, sem que isso represente uma não planejada oscilação no nível de risco.

Estabelecer procedimentos em transações corporativas, operar por meio de regras de restrições e controle de acesso, criar hierarquias de responsabilidades, métodos de reação a eventuais falhas ou vulnerabilidades e, acima de tudo, ter um padrão no que se refere à segurança da corporação, entre outras, são as razões que levam a criação de métodos de avaliação de riscos para redes corporativas.

Dentre os métodos de avaliação de risco destacam-se:

3.1.1. Árvore de Decisão de Risco

O fator “tolerância” é determinante para que se definam investimentos compatíveis com o bem a ser protegido e principalmente, para que o nível de risco residual esteja dentro da zona de conforto e compatível com a natureza de cada negócio. Segundo o método pode-se:

1. **Rejeitar o risco:** esta opção deve ser considerada quando o risco não está sendo considerado pela estratégia do negócio, uma vez que o custo do controle, ou da contramedida, é superior ao risco ou ao bem a ser protegido.
2. **Aceitar o risco:** esta opção deve ser considerada quando o risco é inerente à natureza e ao modelo de negócio, fazendo parte das operações normais e, portanto, tendo sido previsto na estratégia.

A escolha de aceitar o risco gera outro nível de análise:

- **Evitar:** vontade e viabilidade de se eliminar totalmente a fonte de um risco específico;
- **Transferir:** relação custo-benefício e na viabilidade (disposição e capacidade financeira) de terceiros, para assumir o risco;
- **Explorar:** interesse e possibilidade de se obter vantagens competitivas pelo aumento da exposição e do grau de risco;
- **Reter:** interesse do negócio, considerados custo e tolerância, de garantir a manutenção da exposição e do grau de risco.
- **Mitigar:** necessidade do negócio, considerados custo e tolerância, de diversificar, controlar e reduzir os riscos.

3.1.2. OCTAVE

O OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*), desenvolvido pelo CERT (*Computer Emergency Response Team*) é um método de avaliação de riscos auto direcionado que possui os seguintes objetivos:

- Fazer um balanço das informações críticas, necessidades do negócio, perigos e vulnerabilidades;
- Comparar as atuais práticas de segurança da organização com os padrões atualmente conhecidos;
- Gerenciar e controlar todas as avaliações de riscos da organização;
- Desenvolver uma estratégia de proteção, considerando a política de segurança, gerenciamento administrativo e tecnológico;
- Estabelecer uma equipe multidisciplinar que possa desenvolver a segurança da informação da empresa.

3.1.3. Grau de Proteção de Recursos (GPR)

Outro método para a definição dos recursos a serem priorizados no planejamento para situações de contingência é denominado de Grau de Proteção de Recursos (GPR). Trata-se de uma metodologia mais simples que a anterior e que propõe a pontuação de determinados itens de segurança.

O GPR possibilita responder, por exemplo, se a empresa deve investir em um backup do equipamento do estabilizador ou no backup do servidor de arquivos.

Para o cálculo do GPR são levados em conta três itens considerados de importância relevante para análise, sendo:

$$\text{GPR} = [(P * 2) + (B * 3) + (I * 5)] / 10$$

Onde:

P - Possibilidade da indisponibilidade do recurso. Possui peso 2. Para P, são as possibilidades:

- 0 - praticamente impossível;
- 2 - improvável;
- 4 - possível, porém nunca ocorreu;
- 6 - possível e já ocorreu uma vez nos cinco anos;
- 8 - possível e já ocorreu mais de uma vez nos últimos cinco anos;
- 10 - possível e já ocorreu mais de uma vez no último ano.

B - Existência atual de recursos alternativos ou procedimentos alternativos. Possui peso 3. Para este item, os valores possíveis são:

- 1 - existe recurso alternativo testado e funcionando;
- 4 - existe recurso alternativo e foi testado / utilizado no último ano;
- 6 - existe recurso alternativo, porém nunca foi testado / utilizado;
- 8 - existe recurso alternativo parcial;
- 10 - não existe recurso alternativo.

I - Impacto no ambiente computacional ou no ambiente de negócio. Possui peso 5. Escala de valores variando em:

- 1 - não impacta usuário final;
- 2 - impacta o ambiente batch e de desenvolvimento;
- 3 - impacta o ambiente batch de apoio. Ex: passagem para a produção;
- 4 - impacta o ambiente on line de desenvolvimento;
- 6 - impacta o ambiente batch de produção;
- 7 - impacta parcialmente usuários e clientes;
- 10 - impacta grande parte (ou todos) os usuários e clientes.

Exemplo de aplicação do GPR:

Uma empresa precisa decidir entre investir no backup para o sistema UPS (*Uninterruptible Power Supply*) que atende as estações de trabalho ou para o servidor de arquivos. A indisponibilidade do recurso servidor de arquivos já ocorreu pelo menos uma vez nos últimos cinco anos e não existem recursos alternativos na atualidade, o que causa sérios transtornos aos usuários e clientes. A indisponibilidade do recurso UPS é possível, mas ainda não ocorreu. Para ele existe a possibilidade de alimentar os equipamentos de rede diretamente nas tomadas de energia AC, o que, nesse caso, irá impactar apenas os usuários servidos por esse sistema de alimentação no caso de falta de energia da concessionária.

Para o cálculo do GPR consideram-se:

Cálculo GPR do Servidor de arquivos:

P = 6 (possível e já ocorreu uma vez nos cinco anos);

B = 10 (não existe recurso alternativo - backup);

I = 10 (impacta grande parte ou todos os usuários e clientes).

$$\text{GPR} = [(6 * 2) + (10 * 3) + (10 * 5)] / 10 = \mathbf{9,2}$$

Cálculo GPR do UPS:

P = 4 (possível, porém nunca ocorreu);

B = 8 (existe recurso alternativo parcial);

I = 7 (impacto parcial nos usuários).

$$\text{GPR} = [(4 * 2) + (8 * 3) + (7 * 5)] / 10 = \mathbf{6,7}$$

Segundo esse método de avaliação, a empresa deveria investir no backup do servidor de arquivos primeiramente, que obteve um GRP de 9,2 (contra 6,7 do UPS). Entretanto, isto não significa dizer que o sistema UPS não seja importante, pelo contrário, todos os elementos são importantes.