CLEBERMARQUES
WWW.CLEBERMARQUES.COM

Microsoft®
Operations Framework
Práticas comprovadas para excelência operacional

Administração de Segurança - SMF
Security Administration

Última revisão feita em 05 de Outubro de 2007.

Objetivo

Neste artigo veremos os passos necessários para administrarmos a segurança em nosso ambiente de acordo com as recomendações da SMF Security Administration, veremos como é possível organizar as tarefas do dia-a-dia visando um ambiente segurado e gerenciado, boa leitura para todos.

Introdução

Obs.: Achei melhor deixar alguns termos em inglês mesmo porque na maioria das vezes iremos trabalhar com eles desta forma no mercado.

Considerado como um processo crítico em um ambiente de TI a Security Administration - Administração de Segurança, tem a responsabilidade de gerenciar e proteger um ambiente, evitando brechas de segurança e falhas no ambiente que possam ocasionar em perda de informação, seja por problemas, negligência ou até roubo de dados.

Durante a rotina do dia-a-dia a segurança deverá ser considerada uma acompanhante de todos os processos, incluindo o gerenciamento e a mitigação de riscos, baseados na tecnologia utilizada pela organização, gerenciamento de pacotes e atualizações, gerenciamento de incidentes, auditoria e detecção de invasão. Uma política de segurança deve ser definida e seguida com o apoio de outra SMF que veremos mais adiante no quadrante de Otimização, a Security Management.

Entre outros objetivos podemos destacar que esta SMF deve garantir a confidencialidade dos dados onde ninguém deve ter acesso às informações sem autorização, em paralelo a integridade destes dados deve ser assegurada também uma vez que os usuários autorizados devem sentir-se seguros quanto à precisão das informações fornecidas e que nenhuma modificação imprópria foi feita. Logo os dados devem estas disponíveis para que os usuários autorizados possam acessá-los sempre que necessário. Com o intuito de criar e manter um ambiente seguro nossos níveis de segurança deverão se estender entre segurança pessoal segurança de aplicações, segurança de sistema operacional, segurança de hardware e rede e afins.

Definições Importantes

Para entendermos melhor este artigo e a documentação oficial para esta SMF vamos conhecer algumas definições importantes que também são recomendadas pela Microsoft na própria documentação do MOF, lembrando também que mesmo algumas definições sendo as mesmas encontradas no mercado muitas delas são feitas com base nesta SMF.

> Access control: Controle aplicado ao acesso de usuários a determinados objetos e sistemas, privilégios concedidos para executar determinadas tarefas.
>
> Authentication: Método utilizado para identificar os usuários em um sistema, pode ser feito através de senhas, Smart Card, biometria e outros.

Authorization: Processo que verifica quais os direitos e permissões um usuários tem para acessar recursos em um domínio.

Confidentiality: Método que ajuda garantir que apenas os usuários autorizados podem acessar determinada informação ou recurso de rede.

Digital Certificate: De uma forma simples e generalizada o certificado digital é uma estrutura de dados que contem chave publica e privada utilizadas para autenticações.

Identification: É a forma de reconhecer um usuário de forma exclusiva em um sistema, por exemplo, a Identification é uma chave e o Access control é a fechadura, apenas se as duas se encaixarem perfeitamente é que o acesso será permitido.

Integrity: Um método que garante que os dados não foram modificados ou perdidos durante sua transmissão através da rede, ou seja, método que assegura que os dados estão íntegros e não foram adulterados por algum interceptor.

Nonrepudiation: Um conceito de segurança que garante o envio e/ou o recebimento de uma mensagem, por exemplo, para que nenhuma das partes venha a negar o envio ou o recebimento de tal informação posteriormente.

Public Key Infrastructure (PKI): Um sistema de certificados digitais de uma autoridade certificadora, por exemplo, que segue leis, políticas e padrões.

Virtual Private Network (VPN): Uma forma de estender a rede privada de uma empresa permitindo acesso remoto através de uma rede pública como a internet.

Descrição de Processos e Atividades

Para colocarmos em prática as sugestões do MOF para a Administração de Segurança devemos seguir os passos descritos abaixo onde cada etapa vai elevar a segurança de nosso ambiente em um degrau rumo a excelência da nossa operação, mas uma vez não teremos um ciclo de vida para seguir, mas precisaremos manter a idéia de que estes passos são essenciais para alcançarmos o nível de segurança pretendido.

Identification
Nesta primeira etapa teremos que criar padrões de identificação para todos os usuários dos sistemas. O ideal aqui é seguir uma política definida que ao mesmo tempo seja prática e segura, criando IDs que identifiquem cada um dos usuários de forma única e intuitiva. Geralmente esta tarefa se aplica à administração do Active Directory e a Microsoft disponibiliza em seu site documentos que comentam as melhores práticas para se criar usuários de acordo com a quantidade de funcionários entre outros. Logo esta tarefa pode, e deve ser estendida para a identificação em outros sistemas quando for o caso dos mesmos não se integrarem ao AD.

Authentication
Nesta segunda etapa deveremos utilizar autenticação para provar aos sistemas de que o usuário é realmente quem diz ser, em conjunto com a primeira etapa, Identification, a Authentication completa a dupla que é considerada como Usuário e Senha, respectivamente. Nesta fase devemos definir como nossos usuários serão autenticados nos sistemas de nosso ambiente, seja por senhas, Smart card ou biometria. Nos casos mais comuns são utilizadas senhas e devemos ter uma política para criá-las, geralmente seguindo senhas fortes e complexas.

Access control
Nesta terceira etapa nossa tarefa será controlar o acesso dos usuários identificados e autenticados em nossos sistemas, seguindo o princípio de que os usuários deverão ter acesso apenas aos recursos necessários para que os mesmo executem suas atividades do dia-a-dia e nada mais. Um controle efetivo deve ser feito para que garanta que ninguém no seu ambiente tem acesso a algo que não deve.

Confidentiality
Nesta quarta etapa devemos garantir a confidencialidade das informações e para isso, em conjunto com o controle de acesso, poderemos utilizar meios de criptografia para guardar alguns dados em nosso ambiente. Seja utilizando métodos de chave privada (Private Key Encryption) ou pública (Public Key Encryption e PKI), sistemas de arquivos para acesso dos recursos através da rede ou ainda Firewall e filtros de pacotes para acesso remoto via VPN, por exemplo.

Integrity
Nesta quinta etapa deveremos definir mecanismos para garantir que os dados transferidos pela rede não foram modificados ou perdidos parcial ou completamente, e com isso garantir que a pessoa que disponibilizou determinada informação não foi um invasor ou interceptador. A identificação, autorização e o controle de acesso trabalham juntos para manter esta integridade, porém nosso ambiente está sucessível a infecções por vírus e spywares, portanto deveremos aqui nos preocupar também em ter uma política de antivírus com softwares instalados e verificações agendadas periodicamente.

Nonrepudiation
Nesta sexta etapa deveremos utilizar este conceito em nosso ambiente com o intuito de garantir que o envio e/ou o recebimento de uma mensagem, por exemplo, foi feito por determinado usuário, impossibilitando que as partes envolvidas venham negar o envio ou o recebimento de tal informação posteriormente. Geralmente são utilizados certificados digitais ou criptografia passa assinar o envio de e-mails.

Auditing
Esta sétima etapa pode ser implementada com as funcionalidades de Logs de Auditoria da maioria dos sistemas, com isso podemos saber o que foi feito, por quem foi feito e quando foi feito. Em um domínio o nível de auditoria pode chegar ao ponto de sabermos quem fez uma alteração de determinado arquivo ou acesso algum diretório. O intuito aqui é manter um histórico de ações dos usuários e sistemas para quando for preciso provar alguma ação, logo deveremos planejar, implementar e testar um sistema de auditoria em nosso ambiente de TI.

Atenção: Vale lembrar que cada uma das etapas descritas acima oferece muito mais detalhes do que os que vimos aqui, porém detalhar o processo não é o intuito agora, com este artigo nós devemos entender basicamente como funcionam estes passos, mas futuramente iremos estudar estas recomendações na prática, para isso continuem acompanhando os artigos.

Logo abaixo podemos ver o diagrama que representa o fluxo citado acima, os processos neste caso apresentam um início, meio e fim, veja:

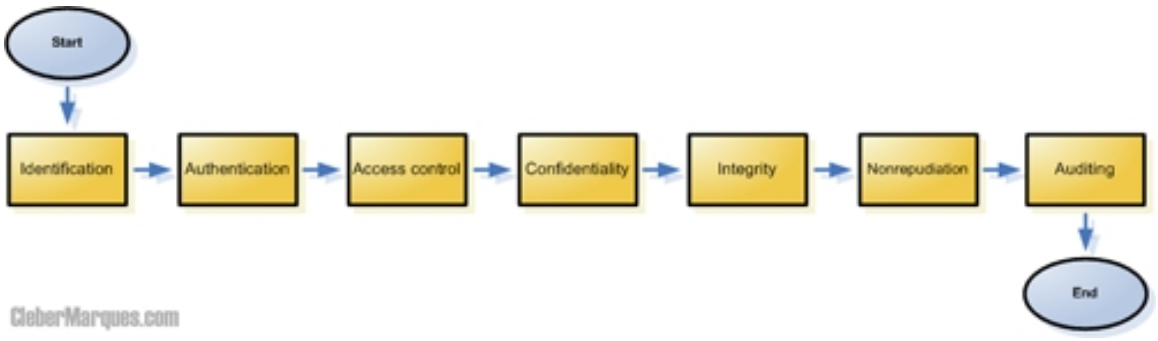

Figura 1 – Fluxo de processos da SMF Security Administration.

Com as novas tecnologias desenvolvidas pela Microsoft temos muito mais alternativas do que antes para nos apoiar na resolução dos passos descritos acima, um bom exemplo é o System Center, uma família de soluções de gerenciamento de TI que nos ajuda planejar, implantar, gerenciar e otimizar de forma pró-ativa nosso ambiente, temos também o SMS, MOM, ISA, Windows Server 2003 o 2008 entre outros, mas este é assunto para um próximo artigo.

Conclusão

Garantir a segurança de nosso ambiente não é tarefa fácil, mas com as práticas recomendadas aqui este processo se torna bem mais intuitivo, logo aprendemos que desde a identificação de um usuário até a forma com que ele se conecta remotamente em nossa rede deve seguir padrões que visam manter um alto nível de segurança para as informações. Na seqüência de nossos estudos vamos entender como funciona o Monitoramento e Controle de Serviços, até o próximo artigo, muito obrigado.

Bibliografia

Referências utilizadas na elaboração deste artigo:

1. Microsoft. www.microsoft.com
2. Microsoft Brasil. www.microsoft.com.br
3. Documentação oficial do MOF. www.microsoft.com/mof

Escreveu,

Cleber Marques
contato@clebermarques.com

Sexta-feira, 05 de Outubro de 2007.