SEGURANÇA DA INFORMAÇÃO: UM ESTUDO SOBRE FERRAMENTAS DE SEGURANÇA PRESENTES NO WINDOWS SERVER

INFORMATION SECURITY: A STUDY ON SECURITY TOOLS IN THE WINDOWS SERVER

Edvaldo Ferreira do Nascimento[1]

RESUMO

O presente artigo trata da segurança da informação, mais precisamente das ferramentas de segurança existentes no Windows Server 2008. Para tanto, é dada uma explicação sobre segurança da informação, bem como as ameaças existentes e os diversos aspectos que um sistema de informação ou rede de computadores devem levar em consideração para se ter um sistema de segurança mais eficiente e menos propenso a invasões ou sabotagens, seja por parte de programas maliciosos, seja por pessoas mal intencionadas que verificam falhas de segurança pra se infiltrarem e assim obterem informações privilegiadas. Durante o trabalho algumas das principais ferramentas de segurança existentes são abordadas, ao final uma pequena análise sobre a importância de se estar sempre atualizando e buscando novas ferramentas que auxiliem na segurança da informação em ambientes profissionais.

PALAVRAS-CHAVE: Informação. Segurança. Ameaças. Ferramentas. Rede.

INTRODUÇÃO

Informação, o bem mais precioso nos dias atuais e também uma fonte de problemas com falhas de segurança. Segundo Junior (2009), existem os seguintes tipos de informação: Armazenada: são considerados dados armazenados os que residem em notebooks, desktops e servidores; Em movimento: são considerados dados em movimento os que residem em *pen drives*, *smartphones*, CDs e e-mails; Em uso: são considerados dados em uso os que se encontram em estado de processamento (sistemas de *e-commerce*, bancos de dados, ERPs etc.). Informações estratégicas são os principais alvos de concorrentes e invasores. Segurança da informação está ligada à proteção de informações e dados com o intuito de preservar o valor que possuem para uma organização ou indivíduo. Para Junior (2009), elaborar e garantir os critérios de proteção às informações contra fraudes, roubos ou vazamentos das empresas são responsabilidades dos gestores e analistas de segurança da informação. Os administra-

[1] Fatec Taquaritinga. Graduado em Processamento de Dados pela Fatec Taquaritinga. Graduando em Sistemas para Internet pela Fatec Taquaritinga. Pós-Graduando em Gestão da Produção pela Fatec Taquaritinga. Endereço: Rua Osmar Mantovani, 57, Jardim Santo Antônio, Taquaritinga – SP. Telefones: (16)92692832 / (16)32536655. Email: edvaldofdn@gmail.com.

dores de redes devem estar constantemente atualizados com relação às ferramentas que auxiliam na proteção das redes de computadores e sistemas operacionais servidores.

Alguns pontos devem ser levados em consideração no que diz respeito à segurança e disponibilidade de informações:

- Definição de planos de atualização e instalação de novos aplicativos no ambiente;
- Definição de políticas e formas de uso da rede;
- Desativação de tudo o que não for necessário em servidores e aplicações;
- Prevenção e detecção à rede de computadores como monitoração e controle da rede;
- Ajuste fino de servidores e aplicações;
- Atenção com o gerenciamento de identidades e controles de acesso à rede;
- Plano de contingência e um plano para recuperação de desastres.

O presente trabalho aborda algumas das diversas ferramentas utilizadas em servidores que utilizam Windows Server, mais precisamente soluções para Windows 2003 Server e Windows 2008 Server.

1. Tipos de ameaças

De maneira geral, risco é qualquer ameaça que possa causar impacto na capacidade de empresas ou diversos outros órgãos de atingirem seus objetivos de negócio. Em tecnologia da informação risco é igual à ameaça.

As vulnerabilidades podem ser relativas às pessoas, tecnologias ou processos. Os eventos de segurança são resultados de determinadas ameaças que exploram essas vulnerabilidades. A tabela 1 mostra a terminologia usada na Segurança da Informação, em seguida a tabela 2 trata sobre as categorias de ameaças:

Tabela 1 – Terminologia

Termo	Definição
Vulnerabilidade	*Software, hardware*, precariedade no procedimento, um recurso ou configuração que pode ser ponto fraco explorado durante um ataque. Também chamado de exposição.
Ataque	Uma tentativa de um agente de ameaça aproveitar as vulnerabilidades com propósitos indesejáveis.
Contramedida	As configurações de *software*, *hardware* ou de procedimentos que reduzem o risco em um ambiente e computador. Também denominada salvaguarda ou atenuação.
Ameaça	Uma fonte de perigo.
Agente de ameaça	A pessoa ou processo que ataca um sistema através de uma vulnerabilidade de uma maneira que viola sua diretiva de segurança.

Fonte: http://www.slideshare.net/khaotikuz/segurana-da-informação-com-windows-server (2011)

Tabela 2 – Categorias de ameaças

Termo	Definição
Spoofing de identidade	Obtenção de acesso ilegalmente e uso das informações de autenticação de outra pessoa, como nome de usuário ou senha.
Violação com dados	Modificação mal-intencionada dos dados.
Repúdio	Associado aos usuários que negam a execução de uma ação, sem possibilidade de provar o contrário. (Não-repúdio refere-se à capacidade de um sistema contra atacar as ameaças de repúdio, inclusive as técnicas como assinar uma encomenda como recebida de modo que o recibo assinado possa ser usado como prova).
Divulgação de informações	A exposição de informações a indivíduos que não possuem acesso a elas, como acessar arquivos sem ter direitos apropriados.
Negação de serviço	Uma tentativa explícita de evitar que usuários autorizados utilizem um serviço ou um sistema.
Elevação de privilégio	Quando um usuário sem privilégios obtém acesso privilegiado. Um exemplo seria um usuário sem privilégio que consegue uma forma de ser acrescentado ao grupo de usuários com privilégios.

Fonte: http://www.slideshare.net/khaotikuz/segurança-da-informação-com-windver (2011)

Na tabela 3 há uma relação dos principais agentes de ameaças existentes tanto para servidores e redes corporativas, quanto para computadores e redes domésticas.

Tabela 3 – Agentes de ameaças

Termo	Definição
Vírus	Um programa de invasão que infecta os arquivos inserindo cópias de código de duplicação automática e apaga arquivos críticos, faz modificações no sistema ou efetua outra ação para causar danos aos dados do computador ou ao próprio computador. Um vírus se anexa a um programa de *host*.
Worm	Um programa que se duplica, frequentemente tão prejudicial quanto um vírus, e pode se espalhar de um computador a outro sem infectar os arquivos.
Cavalo de Tróia	O software ou e-mail que se apresenta como útil ou benigno, mas que de fato executa uma finalidade destrutiva ou fornece acesso ao invasor.
Rootkits	Estes programas miram o controle de um sistema operacional sem o consentimento do usuário e sem serem detectados. Um grande mérito é conseguirem se esconder de quase todos os antivírus existentes devido ao seu código avançado de programação.

Spyware	No começo, os *spywares* monitoravam páginas visitadas e outros hábitos de navegação e informavam os autores. Porém, com o tempo, os *spywares* também foram utilizados para roubo de informações pessoais (como *logins* e senhas) e também para a modificação de configurações do computador (como página inicial do seu navegador).
Phishing Scan ou e-mail bomba	Um e-mail mal-intencionado enviado para um destinatário insuspeito. Quando o destinatário abre o e-mail ou executa o programa, o e-mail bomba efetua ação maléfica no computador.
Atacante ou invasor	Uma pessoa ou organização que executa um ataque.

Fonte: Adaptado de (http://www.slideshare.net/khaotikuz/segurança-da-informação-com-windows-server, 2011)

2. Ferramentas de Segurança no Windows Server

O Windows Server 2008 utiliza uma abordagem multicamadas para implementar a segurança além de oferecer diversas facilidades para se lidar com requisitos de segurança, tais como as políticas de *logs* e acessos aos recursos.

O coração da estratégia de segurança do Windows Server 2008 está no uso de permissões para controlar o que os usuários podem fazer, conforme mostrado na Figura 1. Outros recursos de segurança estão disponíveis com Active Directory, que fornece uma centralização do gerenciamento da segurança da rede que é benéfico para a forte segurança (CABETE, 2009).

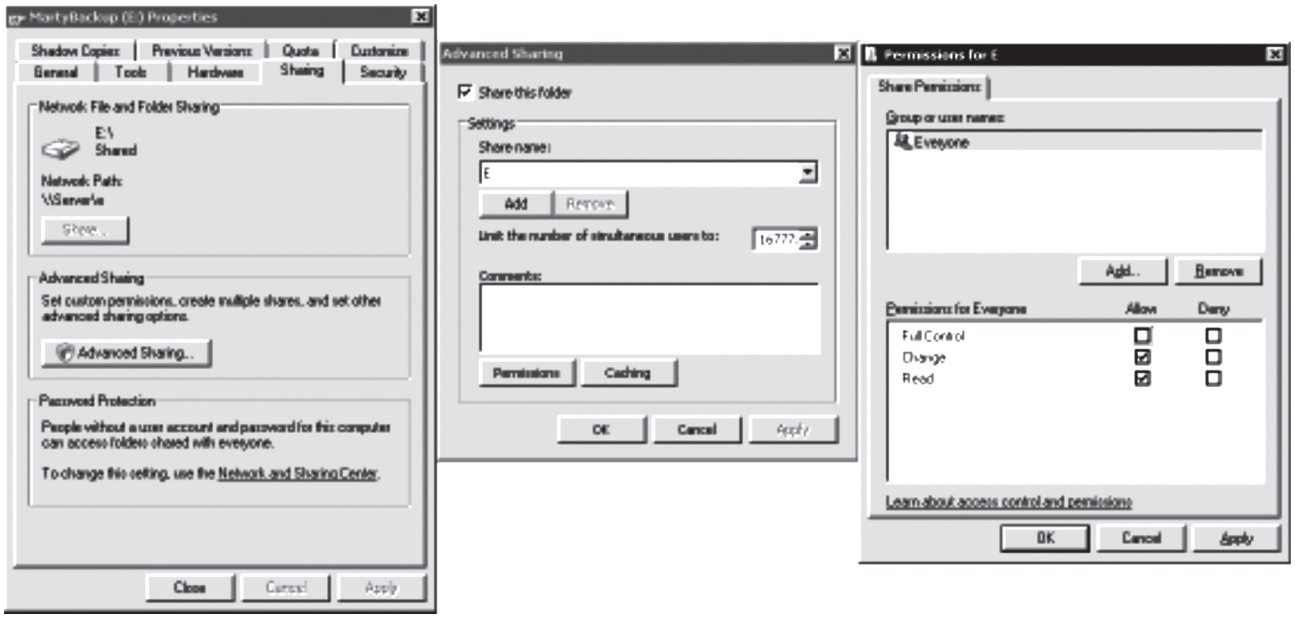

Figura 1 – Aspecto de segurança: definir o que os usuários podem fazer.

Fonte: http://www.olivreiro.com.br/pdf/livros/cultura/2688671.pdf (2009)

2.1. Serviços de Domínio Active Directory

De acordo com a Microsoft (2008), os Serviços de Domínio Active Directory (AD DS) armazenam dados de diretório e gerenciam a comunicação entre usuários e domínios, incluindo processos de *logon* de usuário, autenticação e pesquisas de diretório. Um controlador de domínio do Active Directory é um servidor que executa o AD DS.

2.2. Gerenciador de Autorização

O Gerenciador de Autorização fornece uma estrutura flexível para integrar controle de acesso baseado em função em aplicativos. Ele permite que os administradores que usam esses aplicativos forneçam acesso por meio de funções de usuário atribuídas que se relacionam às funções do trabalho. Os aplicativos do Gerenciador de Autorização armazenam a diretiva de autorização na forma de armazenamentos de autorização nos Serviços de Domínio Active Directory (AD DS) ou em arquivos XML (*Extensible Markup Language*). Esses aplicativos desempenham a diretiva de autorização em tempo de execução. No Windows Server 2008, o suporte para armazenamentos SQL foram adicionados (MICROSOFT, 2008).

2.3. Diretiva de Grupo

A Diretiva de Grupo é uma infraestrutura que permite a implementação de configurações específicas para usuários e computadores.

2.4. Ferramenta Microsoft *Baseline Security Analyzer*

Microsoft *Baseline Security Analyzer* é uma ferramenta fácil utilização desenvolvida para o profissional de TI que ajuda pequenas e médias empresas a determinar o estado de segurança de acordo com as recomendações de segurança da Microsoft e oferece orientação sobre correções específicas (MICROSOFT, 2008).

2.5. Auditoria de segurança

Auditoria de segurança é uma das ferramentas mais avançadas para ajudar a manter a segurança do sistema. Como parte da estratégia de segurança geral, o administrador deve determinar o nível de auditoria adequado para seu ambiente (MICROSOFT, 2008).

2.6. Assistente de Configuração de Segurança

De acordo com a Microsoft (2008), o Assistente de Configuração de Segurança (SCW – *Security Configuration Wizard*) é uma ferramenta de redução da superfície de ataque do Windows Server 2008. O SCW determina a funcionalidade mínima necessária para uma função ou funções de servidor e de-

sabilita a funcionalidade que não é necessária.

2.7. Gerenciamento de Diretiva de Segurança

Diretiva de segurança é uma combinação de configurações de segurança que afetam a segurança em um computador da rede. Por exemplo, as configurações de diretiva de segurança podem controlar quem acessa o computador, quais recursos os usuários estão autorizados a utilizar no mesmo e indica se as ações de um usuário ou grupo são registradas no *log* de eventos. As configurações de diretiva de segurança são definidas por objetos de Diretiva de Grupo que podem ser definidos no nível do computador local ou no nível do domínio. Algumas configurações, como configurações de diretiva de senha, operam somente no nível do domínio (MICROSOFT, 2008).

2.8. Ferramenta de Avaliação de Segurança da Microsoft

Esta ferramenta de avaliação de segurança da Microsoft obtém informações sobre práticas recomendadas para ajudar a melhorar a segurança na infraestrutura de TI.

2.9. *Firewall* do Windows

Segundo a Microsoft (2008), o *firewall* do Windows com Segurança Avançada fornece várias funções em um computador:

- Filtragem de todo o tráfego de IP versão 4 (IPv4) e IP versão 6 (IPv6) entrando ou saindo do computador. Por padrão, o tráfego de entrada é bloqueado, a menos que seja a resposta a uma solicitação de saída anterior do computador (tráfego solicitado), ou seja, especificamente permitido por uma regra criada para permitir o tráfego. Por padrão, todo o tráfego de saída é permitido, exceto para regras de proteção de serviço que impedem os serviços padrão de se comunicarem de maneiras inesperadas. O administrador pode escolher permitir o tráfego com base em números de porta, endereços IPv4 ou IPv6, o caminho e o nome de um aplicativo ou o nome de um serviço que esteja em execução no computador, ou outros critérios.

- Proteger o tráfego da rede entrando ou saindo do computador com o protocolo IPsec para verificar a integridade do tráfego da rede, autenticar a identidade dos computadores ou usuários de envio e recebimento, e opcionalmente criptografar o tráfego para oferecer confidencialidade.

3. Estudo de Caso na Fatec Taquaritinga

A rede da Faculdade conta com servidores Windows e Linux que proveem os mais variados serviços de rede. O estudo de caso aborda os aspectos de segurança citados neste trabalho. Devido a questões de segurança não houve autorização para detalhar e aprofundar cada um dos itens aqui descritos.

Os servidores Windows estão divididos entre três com Windows Server 2008 R2 e cinco com Windows Server 2003 R2, todos interligados e no Domínio.

O servidor que controla o acesso dos usuários na rede tem configurado o Serviço de Domínio Active Directory que gerencia todos os usuários da rede que estejam no domínio sendo um item de segurança muito importante adotado pelos Administradores da rede da faculdade. Cada usuário tem um *login* e uma senha, somente com essas informações em mãos conseguem acessar e usufruir dos serviços da rede.

Os usuários estão divididos em grupos e para cada grupo são dadas permissões diferentes de acesso e uso dos recursos da rede, dependendo do nível de acesso necessário. Por exemplo: o grupo onde estão os administradores tem acesso a todas as configurações dos servidores Windows e das máquinas clientes que estejam no domínio, enquanto que os usuários que se referem ao grupo dos alunos tem somente algumas permissões, não podendo acessar todos os recursos existentes no que diz respeito ao acesso às configurações das máquinas clientes, por exemplo.

Para que estas regras de segurança e acesso às informações e recursos da rede sejam efetivamente implantadas há o uso de Diretivas de Grupos para cada grupo de usuário.

Para auxiliar ao acesso de recursos e restrições na rede existe o uso de scripts de inicialização, onde cada vez que um usuário faz *logon* na rede, esses *scripts* podem fazer, por exemplo, o mapeamento de impressoras, unidades de armazenamento, pastas compartilhadas por grupos de usuários ou usuários.

Os servidores ainda contam com o *firewall* do próprio sistema ativo além de contar com outros firewalls ativos na rede, assegurando uma maior segurança quando diz respeito ao acesso aos servidores ou serviços e áreas restritas.

Cada servidor tem um sistema de antivírus instalado, sendo que a maioria conta com McAfee, um conceituado antivírus.

Cada máquina cliente da rede tem instalado e configurado um software de antivírus, nesse caso esses sistemas de segurança são *free*, ou seja, não necessitam de pagamento para sua utilização.

A rede da Faculdade ainda conta com um servidor de impressão, configurado para que todos os usuários da rede que necessitem usar uma impressora consiga, depois de logado no Domínio (autenticado na rede através do usuário e senha cadastrado no Active Directory), utilizar a impressora que esteja mapeada para seu grupo. Desse modo, o controle de acesso a todas as impressoras ficam centralizadas no Servidor, conferindo maior segurança e controle dos recursos. Este servidor de impressão é implementado via *software*, utilizando-se para tal do Windows Server 2008 R2, com os serviços de impressão e documentos instalados e configurados.

CONSIDERAÇÕES FINAIS

Existem inúmeros conceitos de segurança voltados para servidores que tem como sistema operacional o Windows Server, independente de versão (2000, 2003, 2008), assim como as mais variadas ferramentas de segurança. Um exemplo, os sistemas de antivírus, estes existem e trabalham junto com as soluções já embutidas no Windows, devem estar sempre atualizados e otimizados de acordo com as necessidades de cada administrador ou instituição, seja ela pública ou privada.

Este artigo se propôs a mostrar as ferramentas de segurança do próprio Windows Server, mais precisamente o Windows Server 2008, que até o momento é o mais atual.

Vale ressaltar que é importante conhecer todas as ferramentas disponibilizadas pela Microsoft deixando-as sempre atualizadas e bem configuradas, bem como estar sempre pesquisando ferramentas de terceiros que auxiliam ou solucionam problemas não detectados pelas ferramentas internas do Windows.

Regras de segurança simples devem ser constantemente revistas e colocadas em prática como: regras de criação de senhas; troca de senhas periodicamente; políticas de acesso aos dados e serviços da rede; cuidados para não deixar expostos dados importantes sobre as estruturas das redes e servidores. Informações essas que podem ser uma falha enorme de segurança podendo comprometer todo o esquema de segurança adotado pelo administrador da rede.

ABSTRACT

This article deals with information security, more specifically, existing security tools in Windows Server 2008. Therefore, it is given an explanation about information security and existing threats and the various aspects that an information system or computer network should take into consideration to have a security system more efficient and less prone to invasion or sabotage, whether by malicious programs, whether by malicious people to check security holes to infiltrate and thus obtain privileged information. Throughout the work some of the main existing security tools are discussed. At the end a little analysis on the importance of being always updating and searching for new tools that help information security in the professional environments.

KEYWORDS: *Information. Security. Threats. Tools. Network.*

REFERÊNCIAS

AMOROSO, D. **Aprenda as diferenças entre vírus, *trojans, spywares* e outros**. Tecmundo, 2008. Disponível em: < http://www.tecmundo.com.br/853-aprenda-as-diferencas-entre-virus-trojan-spywares-

-e-outros.htm#ixzz1azvFOEfn /> Acesso: 15 out. 2011.
CABETE, C. **O ambiente do Windows Server 2008**. O livreiro, 2009. Disponível em: < http://www.olivreiro.com.br/pdf/livros/cultura/2688671.pdf /> Acesso: 16 out. 2011.
FONTOLAN, C.; MILAN, R. **Windows Server 2008 – Windows *Firewall with Advanced Security*.** Fórum do Badoo, O melhor fórum brasileiro de ajuda ao usuário *Windows,* 2008. Disponível em: < http://www.babooforum.com.br/forum/index.php?/topic/639804-artigo-windows-firewall-com-config-avancadas-de-seguranca/pdf />. Acesso em: 17 out. 2011.
HOLME D.; THOMAS O**. Administração e Manutenção do Ambiente *Microsoft Windows Server* 2003.** Porto Alegre: Bookman, 2006.
JUNIOR, M.V.S. **O que é Segurança da Informação?** *Webinsider* - Tecnologia, 2009. Disponível em: < http://webinsider.uol.com.br/2009/09/23/o-que-e-seguranca-da-informacao /> Acesso: 15 out. 2011.
LIMA, G. **Segurança de Informação com Windows Server.** *Slideshare, Present Yourself*, 2011. Disponível em: < http://www.slideshare.net/khaotikuz/segurana-da-informao-com-windows-server /> Acesso: 16 out. 2011.
MICROSOFT. **Avaliação e Gerenciamento de Configuração Segura.** Microsoft – TechNet, 2008. Disponível em: < http://technet.microsoft.com/pt-br/library/cc755148%28WS.10%29.aspx /> Acesso: 16 out. 2011.
MICROSOFT. **Ferramentas de Segurança.** Microsoft – TechNet, 2010. Disponível em: < http://technet.microsoft.com/pt-br/library/cc722416%28WS.10%29.aspx /> Acesso: 15 out. 2011.
MICROSOFT. ***Firewall* do Windows com Segurança Avançada.** Microsoft – TechNet, 2008. Disponível em: < http://technet.microsoft.com/pt-br/library/cc772589%28WS.10%29.aspx /> Acesso: 17 out. 2011.