MECANISMOS PARA QUEBRA DE POLITICAS DE ACESSO

Max Victor Henriques Corrêa[1]; Roitier Campos Gonçalves[2]

[1]Graduando em Análise e Desenvolvimento de Sistemas pelo Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro – IFTM Campus Paracatu, Paracatu, MG, Brasil.
maxvictorhc@gmail.com
[2]Professor, IFTM – Campus Paracatu. roitier@iftm.edu.br

Resumo
Este trabalho busca discutir e analisar o comportamento e uso de ferramentas que buscam quebrar de alguma forma as políticas de segurança implementadas em uma rede para o acesso de dispositivos, seja por invasão, desvio de pacotes ou requisição indevida. Serão abordadas as técnicas mais comuns para estes fins e como mitigar essa prática, serão exemplificadas condutas comportamentais que tornam o sistema de segurança vulnerável. Por fim busca-se fazer deste uma boa fonte de consulta para o entendimento destas políticas, técnicas e ainda ser utilizado como subsídio para a criação de uma rede segura.

Palavras-chave: Segurança, Política, Rede, Vulnerabilidade, Conexão.

MECHANISMS FOR BREAK ACCESS POLICIES

Abstract
This work seeks to discuss and analyze the behavior and use of tools that seek to break in some way the security policies implemented in a network for the access of devices, be it by invasion, packet diversion or improper request. The most common techniques for these purposes will be addressed and how to mitigate this practice will be exemplified behavioral behaviors that make the security system vulnerable. Finally, it is sought to make this a good source of consultation for the understanding of these policies, techniques and still be used as a subsidy for the creation of a secure network.

Keywords: Security, Politics, Network, Vulnerability, Connection.

1 Introdução

A tempos atrás quando ainda se usavam papéis para guardar dados importantes a segurança era facilmente aplicada apenas guardando os documentos em locais seguros. Após o uso de tecnologias e digitalização dos dados as estruturas de segurança se sofisticaram trazendo recursos de controles mais rígidos e centralizando as informações, as empresas começaram a ter grandes computadores com acessos restritos onde somente pessoas específicas podiam utiliza-los. Em pouco tempo todos possuíam computadores pessoais conectados ao mundo inteiro, as questões de segurança se tornaram mais complexas e traziam consigo a necessidade de se desenvolverem para suprir o grande volume de dados e pessoas que estavam conectadas, paralelamente os dados digitais adquiriram importância para a sobrevivência de grandes empresas e instituições.

Para CAMPOS, (2007, p. 21) "A informação é elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor". Firma-se então a importância da informação dentro das instituições. Fica claro que na sociedade virtual as informações são consideradas patrimônio vital de qualquer organização, porém ao mesmo tempo é considerada um grande risco pois com tantas pessoas conectadas a mesma grande rede chamada de *internet* fica o grande alerta a todos que a segurança da informação é mais necessária que nunca, tornando-se assim ponto crucial dentro das empresas.

Segundo TORRES (2001, p.5), "As redes de computadores surgiram da necessidade da troca de informações, onde é possível ter acesso a um dado que está fisicamente localizado distante de você", podemos concluir que os dados são acessados remotamente, basta possuir as instruções e privilégios para isso, uma vez que do lado da máquina a verificação de autenticidade é vista através de um identificador.

O objetivo deste trabalho é apresentar as técnicas utilizadas para quebra de políticas de acesso a redes, boas práticas em segurança para qualquer pessoa que esteja em um ambiente conectado a redes, buscando informar e capacitar os profissionais da área a lidarem com a segurança.

2 Definições e conceitos

Para a Norma ABNT NBR ISO/IEC 27002 no item 01. Introdução apresenta a seguinte definição para o assunto:

> "A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (ver OECD Diretrizes para a Segurança de Sistemas de Informações e Redes). "

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao 16 negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio. (ABNT NBR ISO/IEC 27002).

Para os estudos correlacionados a segurança da informação é importante deixar explicita a diferença entre dados e informação. Desta forma, Miranda (1998) estabeleceu alguns conceitos, com o objetivo de padronizar um referencial teórico sobre a variedade de conceitos, de forma a padronizar um entendimento sobre o assunto. Adotou-se os resultados dessa pesquisa para estabelecer os seguintes conceitos:

- **Dado** é conjunto de registros conhecidos, organizados, resultado da experiência ou observação de algum fenômeno ou acontecimento dentro de um sistema ou conjunto de instalações;
- **Informação** são dados organizados, padronizados e estruturados de modo a fornecer algum sentido, sendo subsídio útil para tomadas de decisões. Segundo Teece (1998) a informação sem um contexto raramente é conhecimento;
- **Conhecimento especifico** é o conjunto de informações já identificadas e que caracteriza o saber disponível sobre um tema especifico;
- **Sistema de informações estratégicas** é o conjunto de ferramentas informatizadas que permite o tratamento dos dados coletados pelo monitoramento estratégico, transformando em informações e agregando conhecimento, a fim de que se constitua insumo para a inteligência estratégica;
- **Sistema especialista** é a ferramenta informatizada que agrega o conhecimento de especialistas ao processamento de informações que suportam a tomada de decisão.

No contexto desse trabalho, visa-se acrescentar o foco da informação para os objetivos estratégicos estabelecidos por uma instituição, empresa ou organização. As informações, de vital importância para uma empresa, devem ser preservadas afim de manter a integridade dos dados estratégicos da mesma, para isso faz-se necessário a implementação de políticas.

3 Aspectos legais, políticas e procedimentos de segurança

3.1 Legislação sobre Segurança da Informação e Comunicação

A segurança da informação possui um âmbito enorme de políticas para o cumprimento e mantimento da integridade dos dados. Loureiro (2008) afirma que "A segurança da informação é um assunto de extrema relevância e ainda não possui leis suficientes para ser tratado com toda a complexidade que ele requer. É necessário estabelecer regulamentações para segurança da informação, para políticas nacionais e internacionais relativas ao assunto, para a questão de infraestrutura de chaves-públicas, e para o direito penal voltado a crimes digitais. ", desta forma fica clara a necessidade de se investir nesse aspecto dentro das empresas.

3.2 Políticas de Acesso

Para Ferreira (2003) as políticas, padrões e procedimentos de segurança da informação fornecem melhor direcionamento para implementações técnicas e expressam os anseios da alta direção em decidir na destinação do uso da informação, quem pode acessá-los. Essas políticas devem servir de direcionamento para as ações técnicas que serão tomadas dentro de uma empresa.

Serão apresentados conceitos importantes sobre controles de acesso que utilizam a informática para armazenamento, geração ou divulgação de informações, políticas de segurança e informação das comunicações. Uma Política de Segurança da Informação e das Comunicações tem por objetivo estabelecer diretrizes, critérios e procedimentos para a segurança, tratamento, controle e proteção dos dados, informações e conhecimentos produzidos, armazenados ou transmitidos, por qualquer meio pelos sistemas de informação.

Para os fins dessa política, considera-se acesso lógico como um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizados feitos por pessoas ou programas de computador. Os recursos que devem ser protegidos incluem aplicativos, arquivos de dados, utilitários e o próprio sistema operacional. Serão apresentados abaixo os motivos pelos quais esses devem ser protegidos. O acesso indevido ou por parte de pessoas, softwares ou computadores remotos não autorizados pode ser usado para alterar as funções e a lógica do programa trazendo dados falsos ou desviando as informações para outro destino. Os arquivos de dados, bases de dados e registros devem ser protegidos afim de evitar que sejam apagados ou alterados como um

arquivo de configuração do sistema, dados de uma folha de pagamento em uma empresa ou estratégias de negócio. Editores de texto, compiladores, softwares de manutenção, monitoração, diagnósticos ou qualquer utilitário devem ser protegidos da mesma forma pois são as ferramentas utilizadas para alterar os aplicativos, arquivos de dados, configuração e sistemas operacionais, o último é sempre um alvo muito visado pois é onde ficam as configurações do computador, incluindo a segurança. Caso o S.O. esteja fragilizado acaba-se comprometendo toda a segurança dos anteriormente citados.

Arquivos de senhas e de logs são muito visados também por possuírem registros de acessos importantes, caso uma pessoa não autorizada acesse esses dados pode-se obter identificadores (IDs) e senhas de usuários com privilégios, podendo assim, causar danos ao sistema e acessar todos os dados do mesmo, essa pessoa não será barrada por qualquer política de segurança pois está se passando por um usuário com privilégios. Os logs são usados para registrar ações que são realizadas por usuários que tem acesso aos computadores e a rede, estes se tornam ótimas fontes de informações para auditorias ou fiscalizações, estes registram quem está acessando recursos computacionais, aplicativos, arquivos de dados, ou qualquer atividade em um computador.

Alguns mecanismos de segurança ou controles de acessos são implementados com o objetivo de garantir os seguintes pontos:

- Definições para que unicamente os usuários autorizados possuam acesso aos recursos específicos;
- Cada usuário terá acesso aos recursos realmente necessários para a execução de suas tarefas;
- Os acessos aos recursos mais importantes da instituição devem ser monitorados e restritos a poucas pessoas.

Estes podem ser traduzidos como termos de funções, autenticações, gerência e monitoramento de privilégios, com limitações e prevenções de acessos.

3.3 Políticas de segurança

De acordo com o RFC 2196 (The Site Security Handbook), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.

As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se às alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Algumas normas definem aspectos que devem ser levados em consideração ao elaborar políticas de segurança. Entre essas normas estão a BS 7799 (elaborada pela British Standards Institution) e a NBR ISO/IEC 17799 (a versão brasileira desta primeira). A ISO começou a publicar a série de normas 27000, em substituição à ISO 17799 (e por conseguinte à BS 7799), das quais a primeira, ISO 27001, foi publicada em 2005.

Existem duas filosofias por trás de qualquer política de segurança: a proibitiva (tudo que não é expressamente permitido é proibido) e a permissiva (tudo que não é proibido é permitido).

Os elementos da política de segurança devem ser considerados:

- A Disponibilidade: o sistema deve estar disponível de forma que quando o usuário necessitar possa usar. Dados críticos devem estar disponíveis ininterruptamente.
- A Utilização: o sistema deve ser utilizado apenas para os determinados objetivos.
- A Integridade: o sistema deve estar sempre íntegro e em condições de ser usado.
- A Autenticidade: o sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.
- A Confidencialidade: dados privados devem ser apresentados somente aos donos dos dados ou ao grupo por ele liberado.

3.4 Políticas de Senhas

Dentre as políticas utilizadas pelas grandes corporações a composição da senha ou password é a mais controversa. Por um lado, profissionais com dificuldade de memorizar várias senhas de acesso, por outros funcionários displicentes que anotam a senha sob o teclado no fundo das gavetas, em casos mais graves o colaborador anota a senha no monitor.

Recomenda-se a adoção das seguintes regras para minimizar o problema, mas a regra fundamental é a conscientização dos colaboradores quanto ao uso e manutenção das senhas.

- Senha com data para expiração

  Adota-se um padrão definido onde a senha possui prazo de validade com 30 ou 45 dias, obrigando o colaborador ou usuário a renovar sua senha.

- Inibir a repetição

  Adota-se através de regras predefinidas que uma senha uma vez utilizada não poderá ter mais que 60% dos caracteres repetidos, p. ex: senha anterior “123senha” nova senha deve ter 60% dos caracteres diferentes como “456seuze”, neste caso foram repetidos somente os caracteres “s” “e” os demais diferentes.

- Obrigar a composição com número mínimo de caracteres numéricos e alfabéticos

  Define-se obrigatoriedade de 4 caracteres alfabéticos e 4 caracteres numéricos, por exemplo:

  1s4e3u2s ou posicional os 4 primeiros caracteres devem ser numéricos e os 4 subsequentes alfabéticos por exemplo: 1432seuz.

- Criar um conjunto possíveis senhas que não podem ser utilizadas

4. Técnicas de Segurança

4.1 Virtual Private Network (VPN)

Segundo Granja (2014) uma VPN é uma rede privada construída sobre a infraestrutura de uma rede pública, normalmente a Internet, para conectar redes remotas. Segundo o Infopédia a VPN ainda preserva a privacidade através da utilização de “túneis” e mecanismos de segurança. Conclui-se então que com uma VPN pode-se enviar dados entre dois computadores de maneira que emula uma conexão ponto a ponto privada. As VPN têm a possibilidade de rever seus registros on-line. Uma boa VPN tende a evitar o registro, tais como os detalhes. Não é necessário dizer que compromete as atividades do usuário, e o que eles têm feito online não condiz com o propósito principal de usar uma rede VPN.

Para usar uma VPN, você normalmente precisa fazer o download e, em seguida, instalar um cliente VPN, mas os usuários têm a opção de configurar seus computadores ou dispositivos móveis assim de algumas vezes alterar o nível de criptografia. Depois de tudo estiver configurado, toda e qualquer atividade na Internet, independentemente do programa que você

pode estar usando, será encaminhado através da VPN com segurança. O maior problema de um servidor VPN é que eles são relativamente caros. E além disso, algumas VPN podem restringir a navegação.

É fundamental que você escolha um serviço de VPN de qualidade, que não armazena seus dados ou logs de comunicação. Se um órgão governamental exigir que o provedor de VPN revele os logs, os usuários passam a ficar expostos. Além disso, é importante que o serviço de VPN implemente um balanceamento de carga adequado e uma randomização de servidores para que os usuários possam sempre se conectar a um servidor VPN diferente.

Conclui-se que utilizar uma VPN pode propiciar segurança na comunicação através de criptografia e de túneis, isso evita vulnerabilidades contra qualquer tipo de roubo ou interceptação. Essa é uma ótima tecnologia para ser usada em empresas de grande e pequeno porte que possuem filiais em outras partes do mundo. Basicamente é uma maneira mais segura e barata de conectar redes privadas através de uma rede pública.

4.2 Servidor Proxy

É um serviço intermediário entre as estações de trabalho de uma rede e a Internet. O servidor de rede proxy serve para compartilhar a conexão com a 8 Internet, melhorar o desempenho do acesso, bloquear acesso a determinadas páginas

Basicamente é um computador que atua como intermediário entre a Internet e o computador usuário, todo tráfego percorrido através de um servidor proxy será originado a partir do endereço IP dele, e não do computador usuário. Ao contrário da VPN, os proxies não têm recursos para criptografia dos dados que trafegam entre eles, sendo assim, podem aceitar conexões simultâneas de vários usuários ao mesmo tempo.

Existem dois tipos de Proxy, o HTTP e o SOCKS. O primeiro é projetado para interpretar o tráfego a nível HTTP. Isso significa que eles não são capazes de lidar apenas com o tráfego com URLs que começam com SHTTP: // ou http:// , mas eles são igualmente eficazes para navegar na Web, porém, uma vez que esses servidores não fazem nada mais do que lidar com as solicitações HTTP, eles tendem a serem mais rápidos do que seus servidores VPN habituais ou proxies SOCKS.

Os Proxy SOCKS não interpretam o tráfego de rede, isso os torna muito mais dinâmicos, porém mais lentos. A maior vantagem do protocolo SOCKS é que ele suporta qualquer tipo de tráfego de Internet, incluindo SMTP e POP3 para e-mails, bem como FTP e arquivos torrent,

mas uma de suas maiores desvantagens são suas questões de segurança que são mais ou menos as mesmas que o HTTP.
Os Proxy HTTP são mais baratas e são igualmente eficazes em ocultar seu IP de verificações básicas, o que as tornam a opção perfeita para acessar sites com restrição geográfica e criações de conta.

No entanto, os proxies não foram desenvolvidos para proteger todo o seu tráfego de internet, eles normalmente protegem apenas o navegador. Além disso, muitos proxies passam o endereço IP original do usuário para o site de destino, tornando-os inadequados para usuários preocupados com privacidade ou segurança. Finalmente, os proxies devem ser configurados separadamente para cada aplicativo (e-mail, navegador, aplicativo de terceiros) e alguns aplicativos podem não ser compatíveis.

4.3 Tor

O Tor ou "The Onion Router" (Roteador Cebola) é um serviço criado para permitir que as pessoas naveguem anonimamente pela internet. Ele é um sistema descentralizado que permite a conexão dos usuários por meio de uma rede de retransmissões, em vez de uma conexão direta. O benefício desse método é que o seu endereço IP fica oculto nos sites acessados, ao fazer com que sua conexão pule de um servidor para o outro aleatoriamente, essencialmente, perdendo o rastro.

Enquanto seus dados são criptografados em cada um dos nós de retransmissão, o ponto de conexão final na última retransmissão da cadeia pode ser comprometido se o site solicitado não usar SSL. O Tor tem uma desvantagem conhecida de desacelerar consideravelmente a sua navegação devido aos numerosos saltos pelos quais seus dados são retransmitidos. Para aqueles que estão preocupados com os olhos alheios do governo, o Tor foi criado em conjunto com a Marinha dos Estados Unidos e ainda é utilizado por muitos órgãos governamentais. Como o Tor tem sido utilizado por muitos dissidentes políticos, jornalistas e até por criminosos, muitos governos estão atentos aos usuários do Tor. Isso poderia fazer com que você fosse potencialmente marcado como um tipo de criminoso, tendo todas as suas atividades online monitoradas.

5 Conclusões

É necessário estar atento a questões de segurança em qualquer lugar que existam pessoas que se conectem a uma rede, uma vez que dessa forma estamos vulneráveis a ter informações acessadas por pessoas sem autorização.

As políticas de acesso devem ser implementadas buscando obter um nível de controle sob toda a rede, níveis de acesso e usuários devem ser monitorados para mitigar as chances de invasão ou acesso indevido dos dados.

Todo ato de segurança da informação está relacionado com a proteção de dados, buscando preservar o valor que possuem, sendo assim deve-se dar a devida importância para esse aspecto e lidar de forma crítica com o cenário em que serão aplicados os métodos de segurança.

Existem diversos modos de burlar as técnicas de segurança para acessar informações que são importantes, por isso deve-se ter cuidado com as pessoas que manipulam os sistemas e dão acessos aos usuários, grande parte das invasões ocorrem por vazamento de informações internas que facilitam o invasor a decifrar as políticas de segurança implementadas.

Referências

ANGHINONI, I. Uso de fósforo pelo milho afetado pela fração de solo fertilizada com fosfato solúvel. **Revista Brasileira de Ciência do Solo**, Viçosa, MG, v. 16, n. 2, p. 349-353, 1992.

ARAUJO. L. S. **Uso da "Escoria transformada" como corretivo de acidez do solo e fonte de silício, cálcio e magnésio**. 2007. 27f. (Monografia graduação)- Universidade Federal de Uberlândia, Uberlândia, 2007.

BRASIL. Ministério da Agricultura. Secretaria Nacional de Defesa Agropecuária, Laboratório Nacional de Referencia Vegetal. **Análise de corretivos, fertilizantes e inoculantes métodos oficiais**. Brasília, DF, 1983.

TORRES, Gabriel. Redes de Computadores: Curso Completo. 1ª Edição. Rio de Janeiro: Axcel Books, 2001. 664 p.

CAMPOS, A. SISTEMAS DE SEGURANÇA DA INFORMAÇÃO. 2 ed. Florianopolis: Visual Books, 2007.

Associação Brasileira de Normas Técnicas - ABNT. Norma NBR-ISO/IEC 27001:2006.

Associação Brasileira de Normas Técnicas - ABNT. Norma NBR 27002

TEECE, D Capturing value from knowledge assets. California management Review 1998

MIRANDA, A Produção científica em ciência da informação [Editorial]. Ciência da Informação, Brasília, v.27, n.1, p. 5-6, 1998.

LOUREIRO, SC. "Segurança da Informação: Preservação das Informações Estratégicas com Foco em sua Segurança.[Sl], 12 2008. 66 p." Monografia de Conclusão de Curso (Especialização)-Departamento de Ciência da Computação, Instituto de Ciências Exatas, Universidade de Brasília.
NBR 6023

Granja, Luiz Henrique Garcia. "VPN-Utilidade e Aplicações." Termos Técnicos: 108.

VPN in Artigos de apoio Infopédia [em linha]. Porto: Porto Editora, 2003-2016. [consult. 2016-11-09 18:25:38]. Disponível na Internet: https://www.infopedia.pt/$vpn,2