Privacidade nas Organizações [1]

Anderson Lopes Santos [2]
Gilson Pereira
Keyla Cristina

Resumo

Apresentar de forma gerencial e macro, aspectos envolvendo a segurança da informação nos organizações, privadas ou publicas. Apresentar estudo de caso de determinada empresa de atuação no mercado nacional e propor orientação quanto adoção de alguns critérios que podem ser utilizados em um cenário especifico.

Palavras-chave

Segurança, privacidade, Internet, vulnerabilidade, prevenção, e-mail corporativo, política de uso, rede privada virtual.

Abstract

To present of managemental and macro form, aspects involving the security of the information in the pravate or publish organizations. To present study of case of definitive company of performance in the national market and to consider orientation how much adoption of some criteria that can be used in a scene specified.

Keywords

Security, privacy, Internet, vulnerability, prevention, corporative email, politics of use, virtual private network.

1. Introdução

A tecnologia da informação vem há muitos anos interagindo diretamente com as pessoas, conhecidas como usuários(as) ou clientes, sob esta ótica a preocupação com a segurança da informação vem ser tornando uma necessidade latente nas organizações.

Com advento das redes e massificação da Internet e conseqüente disseminação de serviços faz com que as empresas adotem padrões de segurança em suas aplicações.

[1] Trabalho desenvolvido disciplina Segurança da Informação do MBA em Gestão de Sistemas de Informação da UCB, no 1º semestre de 2003.
[2] Todos os autores são alunos do MBA em Gestão de Sistemas de Informação da UCB

2. Visão Geral de Privacidade nas Organizações

A segurança em aplicações dever estar inserida no contexto mais amplo da segurança do ambiente, que inclui segurança de servidores, equipamentos ativos e ate segurança física.

Assim sendo, é de muita importância que o desenvolvedor tenha uma visão mais ampla de aspectos de segurança na INTERNET mundial e especificamente na INTERNET/BR sob aspectos do atual cenário, mantendo noções atuais sobre as estatísticas de ataques e conhecer determinados perfis de certos "profissionais" da área, ressaltando aqui atuação de alguns brasileiros e outros.

3. Segurança em Sistemas Eletrônicos

Sob vários aspectos o nível de segurança de redes no Brasil está equivalente aos praticados no mundo e existem algumas experiências genuinamente nacionais que superam em muito àqueles concorrentes no exterior, inserindo em suas funcionalidades todos os aspectos inerentes ao dado seguro, coeso (ex.: rede bancaria e votação eletrônica, dentre alguns...).

No entanto, em todo o mundo existem uma farta disponibilidade de ferramentas de ataque prontas para uso, que em geral podem ser baixadas gratuitamente da rede mundial e não exigem deste "usuário" nenhum conhecimento prévio ou qualificação especial na área de informática, basta saber clicar um mouse ou reproduzir alguns comandos contidos em milhões de paginas da grande rede.

4. Aspectos de Segurança na Internet

4.1 Via de Acesso ao ataque

O Caderno de informática do Correio Braziliense de 06/Julho/2001 relata o que já é de conhecimento de toda a imprensa mundial, a necessidade de exposição, a tendência á aparição pública ou glamour à fácil exposição destes atacantes com suas "carreiras" ou atividade de segurança.

Dá-se aqui vida aos mitnick, Onel de Guzman, Jerome Heckenkamp dentre muitos outros que travam verdadeiras guerras nas tentativas de quebras de códigos de acessos e/ou iniciam competições para determinação de quem é o melhor nesta pseudo-modalidade.

Importante salientarmos que uma característica marcante a esta competição é que segundo informações, os atacantes brasileiros são os mais atuantes, no entanto, como a qualidade técnica esta em descobrir vulnerabilidades ou criar novas ferramentas esta qualidade técnica então será creditada ao "profissionais" oriundos de paises como Rússia, Romênia, Holanda, Filipinas e EUA.

5. Redes VPN's

5.1 Conceito

Virtual Private Network (VPN), ou Rede Privada Virtual, é uma rede privativa (com acesso restrito) construída sobre a infra-estrutura de uma rede pública, geralmente a Internet.

Como surgiram

O conceito de VPN surgiu da necessidade de se utilizar redes de comunicação não confiáveis (redes públicas) para trafegar informações de forma segura, pois tendem a ter um custo de utilização inferior aos necessários para o estabelecimento de redes proprietárias, envolvendo a contratação de circuitos exclusivos e independentes.

No entanto, não é apenas em acessos públicos que a tecnologia de VPN pode e deve ser empregada.

Como Funciona

Utiliza as mais avançadas tecnologias de criptografia, assegurando privacidade e integridade das comunicações, substituindo com vantagem os links dedicados e de longa distância. Dispensa a implementação de redes independentes que, geralmente, geram os custos.

Características

Permite que as empresas criem uma rede totalmente integrada, conectando escritórios, filiais e fábricas, com tráfego de voz, dados e vídeo.

Garante segurança máxima na comunicação, graças ao exclusivo acesso via backbone.

Pode ser agregada a inúmeros recursos o que tornam o VPN um produto completo e eficiente na redução dos custos corporativos.

Pressupõe que não haja necessidade de modificações nos sistemas utilizados pelas corporações, sendo que todas as necessidades de privacidade que passam a ser exigidas sejam supridas pelos recursos adicionais disponibilizados nos sistemas de comunicação.

Possibilita a medição da qualidade de Serviço sobre múltiplas redes, segregar dados, autenticar usuários e evitar coincidência de IPs.

Funções Básicas

Confidencialidade - Tendo em vista que estarão sendo utilizados meios públicos de comunicação é imprescindível que os dados que trafeguem sejam absolutamente privados, de forma que, mesmo que sejam capturados, não possam ser entendidos.

Integridade - Na eventualidade dos dados serem capturados, é necessário garantir que estes não sejam adulterados e re-encaminhados. Tem de garantir que somente dados válidos sejam recebidos pelas aplicações suportadas pela VPN.

Autenticidade - Somente usuários e equipamentos que tenham sido autorizados a fazer parte de uma determinada VPN é que podem trocar dados entre si; ou seja, um elemento de uma VPN somente reconhecerá dados originados por um segundo elemento que seguramente tenha autorização para fazer parte da VPN.

Técnicas Utilizadas

Modo Transmissão - Somente os dados são criptografados, não havendo mudança no tamanho dos pacotes. Geralmente são soluções proprietárias, desenvolvidas por fabricantes.

Modo Transporte - Somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes. É uma solução de segurança adequada, para implementações onde os dados trafegam somente entre dois nós da comunicação.

Modo Túnel Criptografado - Tanto os dados quanto o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e de destino.

Modo Túnel Não Criptografado - Tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino. No entanto, cabeçalho e dados são mantidos tal como gerados na origem, não garantindo a privacidade.

Protocolos Utilizados

IPSec - conjunto de padrões e protocolos para segurança relacionada com VPN sobre uma rede IP, e foi definido pelo grupo de trabalho denominado IP Security (IPSec) do IETF (Internet Engineering Task Force).

PPTP - Point to Point Tunneling Protocol é uma variação do protocolo PPP, que encapsula os pacotes em um túnel IP fim a fim.

L2TP - Level 2 Tunneling Protocol é um protocolo que faz o tunelamento de PPP utilizando vários protocolos de rede (ex.: IP, ATM, etc.) sendo utilizado para prover acesso discado a múltiplos protocolos.

SOCKS v5 é um protocolo especificado pelo IETF e define como uma aplicação cliente - servidor usando IP e UDP estabelece comunicação através de um servidor proxy.

Tipos de VPN´s

VPN para Intranet

VPN para Acesso Remoto

VPN para Extranet

VPN Frame relay - permite a separação de tráfego por circuitos virtuais. Não provê encriptação e segurança de dados. Baixa velocidade

VPN ATM - Apenas para backbones de operadoras ou grandes bancos, pois é a mais cara (um switch de ATMs custa mais de 6 milhões de dólares). Alta velocidade.

VPN MPLS (multiprotocol label switching) - é uma VPN IP flexível, permite criar uma rede com muitos agentes sem muita complexidade. Não tem padronização e não provê criptografia.

VPN IPSec (internet protocol security) - mais popular. Possui criptografia de dados, permite controle de acesso, integridade e confidencialidade. Montada de fim a fim entre roteadores, firewalls, estações de trabalho e servidores.

Utilização das Virtual Privates Network´s no Brasil

Segundo pesquisa da revista INFORMATIONWEEK Brasil, das 130 empresas pesquisadas 53% afirmaram utilizar a tecnologia e das 100 empresas mais inovadoras em TI 74% de utilização da tecnologia.

O Padrão VPN IP (Internet protocol) é a mais utilizada, e o caso clássico de utilização desta tecnologia e o Projeto SPB (Sistema Brasileiro de Pagamentos), o SBP conta com a proteção e capacidade de interligação da tecnologia.

A rede do SPB permite por meio de VPN IP, protocolo MPLS a comunicação direta entre o Banco Central, as clearings e as Instituições Financeiras (200 instituições ao todo). Varias são as organizações que utilizam esta tecnologia e uma outra grande empresa do cenário nacional usuária deste padrão é a Infraero (Empresa Brasileira de Infra-Estrutura Aeroportuária) que possui desde 2002 algo em torno de 250 conexões autorizadas em vários aeroportos brasileiros e em segmentos de seu interesse e atuação.

6. Estudo de caso (Case) - Empresa X

Quanto maior a visibilidade da organização, maiores possibilidade de ataques. Verifica-se que as áreas de interesses na maioria destas tentativas tem sido a aquisição/controle de cartões de credito e/ou cartões bancários de forma fraudulenta (roubo) e ainda a apropriação indevida do servidor de nomes (DNS) da empresa.

O acesso ao recibo impresso que em tempos remotos eram descartados diretamente ao lixo sem a completa destruição eram os objetos de desejo de qualquer invasor e outra forma de tentativa de invasão são aquelas ações de execução de alguns comandos em sua consoles efetuando a presunção ou simulação de senhas padrões.

6.1 Monitoramento (Case) - Empresa X

Empresa"X"	
Mês ZZZZZZ/2002	
Tentativas Ataques ao ambiente	965
Tentativas Ataques automáticos (70% por Codered,Nimda e variantes)	675
Restante por ataques manuais, buscando vulnerabilidades nos serviços/servidores	290

7. E-mail Corporativo

As empresas sentem a necessidade de verificar todo o conteúdo informacional que transita dentro e fora das suas instalações físicas. O e-mail é uma ferramenta de comunicação muito útil e, por conseqüência, demasiadamente utilizada. Acarreta que tamanha disseminação do uso deste meio de comunicação tornou-se um ponto de difícil controle, não somente em termos de tecnologia, como também, e talvez principalmente, em termos políticos.

Nancy Flynn, diretora executiva do The ePolicy Institute, recomenda que as organizações adotem o que ela chama de "abordagem dos três E´s": Estabelecer a política; Educar a força de trabalho, e; Empregar a política de maneira consistente.

7.1 Definição da política de uso

Toda organização necessita estabelecer de forma clara qual a política de uso aceitável para esta ferramenta para que ela não se torne um problema ao invés de ser uma solução. Não é uma tarefa simples, até porque envolverá também uma mudança de cultura dos seus funcionários.

Uma política de uso tem de ser clara. Termos como "uso impróprio" ou "conteúdo indevido" têm de ser colocados de outra forma para não deixar dúvidas, e estas dúvidas, por sua vez, serão as brechas utilizadas pelos advogados, caso a organização entre com um processo contra seus funcionários com base nestas regras. Vejamos um exemplo clássico: "A empresa XYZ reserva-se o direito de monitorar ou analisar qualquer informação armazenada em seu equipamento ou transmitida através dele". Reservar-se o direito de monitorar é substancialmente diferente de declarar claramente que a empresa de fato monitora. Estabelecer limites e educar os funcionários de tal forma que todos conheçam estes limites também é de fundamental importância para o sucesso da política de uso do e-mail.

7.2. Disseminação da política

Definidas as regras, a organização precisa adotar uma maneira para que todos os seus funcionários, novos e antigos, tomem conhecimento delas. É de vital importância que todos os colaboradores tenham consciência que estarão, ou poderão estar, sendo

vigiados. Que todo o conteúdo que transita na sua caixa de e-mail não é de propriedade dele e sim da organização (desde que tenha sido assim definido).

As pessoas, quando sabem que estão sendo vigiadas, têm mais cuidado com aquilo que utilizam ou fazem, e assim funciona também com o e-mail. Saber que conteúdo pornográfico e piado no e-mail é terminantemente proibido e é motivo de demissão por justa causa pode não suficientemente "assustador" para o funcionário, a não ser que ele saiba que este conteúdo é fortemente vigiado.

7.3. Colocando em prática

Muitos funcionários, que fazem parte da turma que vigia o conteúdo dos e-mails, geralmente têm dificuldade de passar a informação a diante e agem como se nada tivesse ocorrido. Este comportamento, por sua vez, causa uma falha na política que foi implantada e disseminada mostrando aos demais funcionários que não é bem como está escrito, existe um relaxamento. Talvez este seja um dos grandes desafios dos gestores: Definir processos para que a política transcorra de forma natural na empresa.

Ao se disseminar a política de uso na organização, espera-se que ela faça parte da sua cultura, que seja um ato já institucionalizado e que funciona. Para tanto, é importante também não se deixar tudo nas mãos de um grupo de funcionários – equipe de segurança da informação, por exemplo. Automatizar este processo, colocar ferramentas para auxiliar o trabalho da equipe e "desumanizar" um pouco o processo é vital.

Uma coisa é elaborar uma política "sem prisioneiros", que ameaça com sérias conseqüências os funcionários que zombam de suas regras; outra coisa é adotá-las. A política de uso só tem força dentro da empresa na medida em que seus funcionários são devidamente punidos por infringirem suas regras. Uma maneira de garantir que o uso desta política não criará um caos na organização é deixar que todos tomem conhecimento quando os primeiros funcionários começarem a serem punidos com base nesta. Esta é uma maneira muito eficiente de mostrar a todos os funcionários que a organização realmente está vigilante.

8. Principais Vulnerabilidades

Adotar senhas padrões ou facilmente presumíveis tem sido uma das falhas que facilitam as possíveis invasões, assim deve-se proceder a escolha de senhas mais complexas ou duplas senhas.

A preocupação de que o foco é a entrega e confecção do produto deve ser importante mais não menos importante será a ação eficiente de descarte e substituição de senhas utilizadas no desenvolvimento e testes do produto.

A adoção de algoritmos de criptográfica, ou seja, evitar o tráfego de Informações sensíveis constituem-se em ações que serão obstáculos a invasões de sistemas eletrônicos sem criptografia, a localização física do servidor e a substituição dos switchs por hubs são ações de ordem física que também podem fazer a diferença sob os aspectos de segurança.

Não confiar ou não utilizar formulários “escondidos” (hidden forms) em códigos HTML, pois facilmente pode-se editar o código-fonte com ação de desabilitar, no navegador, as linguagem ‘script’ e aqui temos outro caso clássico de invasão, uma vulnerabilidade.

8.1 Prevenção

Para se obter alguma privacidade nas organizações, foram propostos alguns padrões, a conhecida norma ISO/IEC 15.408 que define critérios comuns para prevenir surpresas no desenvolvimento.

Existem algumas orientações para a validação na aplicação ou CGI e não em linguagem (javascript , por exemplo), estabelecer ou adotar filtros para tipos de campos trabalhados na aplicação (numéricos/alfa), evitar as chamadas a rotinas externas tipo “system(),exec()” ou quando não for possível evita-las, manter sob rígido controle e monitoramento..

Promover a substituição de senhas padrão, eliminando as demais, restringindo ao máximo o acesso de usuários remotos (especialmente os que possuem integração do banco com servidores WEB).

9. Conclusão

A área de segurança, assim como todas as demais áreas de desenvolvimento possuem características dinâmicas e exigem atenção constante.

Estabelecer padrões de qualidade e uma cultura em segurança é muito importante, bem como, o uso de tecnologias e políticas adequadamente implantadas.

A adoção de tecnologias integradas com o processo e política de segurança são fatores muito importantes para manter a estabilidade e confiança no ambiente de informação.

10. Referências Bibliográficas

Nelson Murilo
Artigo Técnico “Segurança em Desenvolvimento de aplicações” Fev../03

Argos Consultoria
Srs.. André Calazans e William Guedes - Palestra SENAC - Maio/2003

Information Week
Artigo Técnico “Segurança e mobilidade fazem com que as VPN’s se alastrem pelas empresas - Fev.../2003)

Correio Braziliense
Caderno de Informática - Julho/2001

[http1] http://www.microsoft.com/security

[http2] http://www.microsoft.com/brasil/technet