Guia de Boas Práticas de Segurança para E-Commerce

(Administrador de Infraestrutura)

Versão 10.04.2012

abecs - associação brasileira das empresas de cartão de crédito e serviços
www.abecs.org.br Segurança e Prevenção a Fraude

Realizar negócios através da Internet é uma alternativa de alto valor estratégico para os empresários que optaram por investir neste segmento. Os limites geográficos são removidos e os custos operacionais são consideravelmente menores em comparação com os negócios baseados em lojas físicas.

Este é um mercado que tem se desenvolvido em ritmo elevado e a tendência é que este curso de elevação seja mantido, pois, com o crescimento da economia e as ações do governo federal no sentido de democratizar o acesso a tecnologia se espera um aumento expressivo no volume de novos consumidores na Internet, sobretudo aqueles que recentemente alcançaram a classe média.

Um cenário tão favorável para novos negócios e com alta circulação de dinheiro desperta o interesse de criminosos que buscam tornar seus golpes cada vez mais sofisticados à medida que a tecnologia evolui.

Se proteger desta modalidade de crime é uma tarefa que exige o esforço de todos. No entanto, as pequenas e médias empresas são as que se tornam mais vulneráveis ao crime eletrônico, devido ao fato de que, para manterem custos competitivos, geralmente não possuem profissionais com foco em desenvolver e manter ambientes e sistemas seguros.

Acreditamos que a chave para a proteção do mercado, sobretudo o do comércio eletrônico, reside no compartilhamento do conhecimento. Desta forma, este guia possui o objetivo orientar empresários, profissionais de infraestrutura tecnológica e desenvolvedores de sistemas ligados ao Comércio Eletrônico no sentido de proteger suas aplicações web reduzindo riscos de ataques, comprometimento de informações e fraudes. Serão descritas aqui as formas mais comuns de ataques na Internet e formas de proteção com uma linguagem acessível, de acordo com a atividade desempenhada por cada profissional.

Boa leitura.

O trabalho dos administradores de infraestrutura envolve, na maior parte do tempo, o esforço para manter servidores, estações de trabalho e dispositivos de rede disponíveis. No entanto, deve fazer parte das atividades destes profissionais, a padronização e parametrização dos dispositivos com foco em protegê-los de ataques.

Abaixo estão dispostas as regras para a parametrização de ambientes com foco na segurança das informações.

1. Proteção do perímetro

Ao iniciar o trabalho de proteção de uma plataforma tecnológica se deve definir um perímetro de segurança no qual serão agrupados os dispositivos de acordo com a sua função e interação com informações críticas. A partir do estabelecimento deste perímetro devem concedidas as permissões de acesso adequadas para cada dispositivo. Abaixo as regras para o estabelecimento de um perímetro de segurança:

1.1. Utilize firewalls para segregar as redes do ambiente. Evite usar roteadores para realizar esta função.

1.2. Procure utilizar firewalls com a função de “stateful inspection”.

1.3. Analise o desenho de sua rede criticando se os dispositivos (servidores, switches, etc,) estão devidamente agrupados em redes específicas de acordo com a sua importância para o negócio. Caso estes ativos não estejam segregados desta maneira, considere separá-los. Esta atividade cria zonas de segurança por função, o que limita o alcance de um possível ataque.

1.4. Elabore uma DMZ com o objetivo de abrigar todos os dispositivos expostos à internet. Limite todo o tráfego de entrada somente para a DMZ.

1.5. Concentre os servidores de banco de dados em uma rede apartada, nunca os deixem expostos à internet.

1.6. Segregue através de firewalls os ambientes de desenvolvimento, homologação e produção.

1.7. Estabeleça quais são as portas permitidas para a comunicação entre seus dispositivos e as documente. Esta atividade aumenta o controle e torna formal qual tipo de comunicação é permitida em seu ambiente.

1.8. Evite o uso de portas de comunicação reconhecidamente consideradas como vulneráveis como TELNET e FTP. Prefira soluções com criptografia como SFTP e SSH, quando necessário.

1.9. Determine formalmente quais as pessoas que possuem a função de administrar os firewalls e outros dispositivos de rede.

1.10. Defina um processo formal para a manutenção e alteração de regras nos firewalls. Este processo deve contemplar uma solicitação de mudança para cada regra com a aprovação de pelo menos um gestor.

1.11. Caso possua redes sem fio em seu ambiente, segregue-as através de firewall concedendo somente os acessos necessários para os equipamentos com origem nestas redes.

1.12. Configure os pontos de acesso wireless para usar somente o padrão de criptografia de autenticação WPA2 com chaves longas.

1.13. Nunca utilize o padrão de criptografia de autenticação WEP.

1.14. Proíba qualquer acesso originado na internet que tenha como destino algum equipamento da rede interna.

1.15. Utilize o mascaramento de IP (Network Address Translation - NAT) para todo o tráfego de saída para internet.

1.16. Não utilize senhas padrão de fábrica em nenhum dos equipamentos.

1.17. Configure os dispositivos de rede para gerar logs de todos os eventos realizados com privilégios administrativos.

1.18. Configure os dispositivos de rede para gerar logs de todos os eventos cuja tentativa de acesso resultou em falha.

1.19. Configure os logs para manter os dados de data/hora do evento; identificação do usuário; tipo de evento; indicação de sucesso ou falha e a indicação de qual componente foi alterado ou sofreu uma tentativa de alteração.

1.20. Centralize os logs dos dispositivos de rede e servidores em um servidor com esta função.

1.21. Desabilite a função SOURCE-Routing em roteadores, evitando a possibilidade de inserção não autorizada de rotas nos dispositivos.

1.22. Desabilite a função PROXY-ARP em roteadores, evitando a possibilidade de obtenção não autorizada de informações do dispositivo.

1.23. Instale um software de IPS/IDS e o monitore constantemente.

2. Proteção do Tráfego

Os controles abaixo possuem o objetivo de evitar que informações sensíveis sejam obtidas de forma não autorizada através da captura de dados em trânsito.

2.1. Utilize obrigatoriamente a criptografia SSL V3 impedindo a conexão por meio do uso de versões antigas do SSL. Esta regra é aplicada através da alteração da configuração de seu webserver[1].

2.2. Somente utilize certificados digitais de autoridades certificadoras válidas.

2.3. Monitore a validade do certificado digital e busque adquirir um novo com antecedência à expiração do certificado instalado.

2.4. Somente administre dispositivos utilizando protocolos com criptografia como SSH.

2.5. Somente realize a troca de arquivos entre dispositivos utilizando protocolos com criptografia como SFTP.

2.6. Proíba o tráfego de dados de cartão via e-mail, instant messaging, Skype, etc.

3. Proteção de Servidores e Estações de Trabalho

Os controles abaixo possuem o objetivo de estabelecer padrões para a configuração de servidores e estações de trabalho sob a perspectiva da segurança das informações.

3.1. Sempre que possível, determine, sobretudo na DMZ, uma função por servidor. Manter diversos serviços em um servidor (web server e banco de dados, por exemplo) acarreta na ativação de diversos serviços por máquina, o que pode torná-la vulnerável.

[1] Informações sobre como impedir o acesso ao seu webserver IIS da Microsoft com versões antigas do SSL podem ser obtidas em http://support.microsoft.com/kb/187498 Para servidores Apache, o guia para configuração pode sem obtido em http://httpd.apache.org/docs/2.0/ssl/ssl_howto.html .

3.2. Sempre altere as configurações de qualquer dispositivo antes de instalá-lo em produção evitando manter qualquer configuração de fábrica como usuários e senhas, acessos, etc.

3.3. Desabilite todos os serviços e protocolos desnecessários para a funcionalidade do servidor.

3.4. Estabeleça uma política de senhas da seguinte maneira:

3.4.1. Comprimento mínimo de 8 caracteres;

3.4.2. Período de expiração de no mínimo 45 dias;

3.4.3. Obrigatoriedade de que a senha seja composta de caracteres numéricos e alfanuméricos;

3.4.4. Obrigatoriedade de o usuário, ao compor uma nova senha não utilize nenhuma das quatro senhas anteriores;

3.4.5. Bloquear a conta do usuário após cinco tentativas de acesso sem sucesso;

3.4.6. Manter o usuário bloqueado de acordo com a regra 3.4.5 (acima) por 30 minutos ou até o desbloqueio do administrador.

3.5. A prática de compartilhamento de senhas entre os funcionários deve ser proibida.

3.6. Contas de acesso de serviço devem ser utilizadas somente para o uso em sistemas específicos, nunca devem ser usadas para o logon por usuários.

3.7. Configure os servidores para gerar logs de todos os eventos realizados a partir de usuários com privilégios administrativos.

3.8. Configure os servidores para gerar logs de todos os eventos realizados a partir de usuários de serviço.

3.9. Configure os servidores para gerar logs de todos os eventos cuja tentativa de acesso resultou em falha.

3.10. Configure os logs para manter os dados de data/hora do evento; identificação do usuário; tipo de evento, indicação de sucesso ou falha e a indicação de qual componente foi alterado ou sofreu uma tentativa de alteração.

3.11. Estabeleça mecanismos de controle de acesso para proteger os arquivos de log do acesso não autorizado.

3.12. Defina e documente um padrão de configuração para cada tipo de dispositivo de sua rede.

3.13. Revise os padrões de configuração periodicamente.

3.14. Não utilize softwares não confiáveis em seu ambiente.

3.15. Instale e mantenha atualizado um software de antivírus em todos os computadores que se apliquem.

3.16. Configure o software antivírus para realizar um scan completo em todos os computadores, pelo menos uma vez por semana.

3.17. Realize o controle de acessos, considerando que se deve limitar os acessos ao mínimo necessário para que os empregados e prestadores de serviço realizarem as suas atividades.

3.18. Revise todos dos acessos, no mínimo em periodicidade anual.

3.19. Mantenha todos os sistemas atualizados com as correções do fabricante.

3.20. Somente conceda acesso remoto (através da internet) aos empregados e prestadores de serviço por meio de VPNs.

3.21. Desabilite todos os acessos dos empregados e prestadores de serviço imediatamente após o seu desligamento da empresa ou encerramento do contrato de prestação de serviços.

3.22. Execute scans de vulnerabilidade ao mínimo trimestralmente.

3.23. Estabeleça procedimentos, com periodicidade ao mínimo anual, de teste de intrusão com foco na tentativa de exploração de vulnerabilidades em redes de sistemas operacionais.

3.24. Elimine as vulnerabilidades reportadas em, pelo menos um mês após a detecção.

4. Armazenamento de Dados de Cartão

A Abecs recomenda fortemente que seja analisada a necessidade de se armazenar dados de cartão. Armazenar estas informações acarreta no risco de fraude e em investimentos destinados a proteção destes dados. Se este tipo de informação não é necessária para a continuidade dos processos de negócio de sua empresa, considere sua remoção. Caso contrário aplique as regras abaixo:

4.1. Somente armazene o número do cartão de maneira parcial mantendo somente as quatro últimas posições (ex.: **********1234) ou em modo criptografado.

4.2. Se o nome do portador do cartão e a data de vencimento forem armazenados em conjunto com o numero do cartão estes deverão estar em modo criptografado.

4.3. Não armazene em hipótese alguma as informações do código de segurança

4.4. Estabeleça uma política de expurgo dos dados do cartão em no mínimo um ano.

4.5. Monitore o acesso ao dado de cartão e investigue casos de acessos suspeitos

5. Criptografia

O armazenamento do número de cartão completo em conjunto com o nome do portador e data de vencimento requer o uso de criptografia destas informações. Abaixo os requisitos para a criptografia de dados de cartão.

5.1. Determine um reservatório central para os dados criptografados.

5.2. Obtenha uma solução de criptografia robusta que utilize algoritmos públicos com chaves de no mínimo 128-bits para criptografia simétrica e 1024-bits para criptografia assimétrica.

5.3. Garanta que a informação seja criptografada e decriptada no momento do acesso ao repositório e não haja cache com informações em texto claro em memória não volátil.

5.4. Estabeleça um processo formal de, no mínimo dupla custódia, para a definição das chaves de criptografia.

5.5. Proteja as partes da chave, limitando seu acesso ao menor número de pessoas possíveis.

5.6. Troque as chaves criptográficas pelo menos uma vez por ano ou imediatamente para os casos de suspeita de seu comprometimento.