FACULDADE DE TECNOLOGIA SENAC GOIÁS

SEGURANÇA DA INFORMAÇÃO

Cristhian Lopes de Souza

Matheus do Carmo

Matheus Oliveira

Pablo de Almeida

PLANEJAMENTO EM SEGURANÇA DA INFORMAÇÃO

Olegário Correa da Silva Neto

GOIÂNIA,

2016

Cristhian Lopes de Souza

Matheus do Carmo

Matheus Oliveira

Pablo de Almeida

PLANEJAMENTO EM SEGURANÇA DA INFORMAÇÃO

Relatório apresentado como requisito parcial para obtenção de aprovação na Projeto Integrador na disciplina de Planejamento em segurança da Informação, no curso de Segurança da informação, na Faculdade de Tecnologia Senac Goiás.

GOIÂNIA,

2016

RESUMO

Neste relatório será apresentado um exemplo de planejamento em segurança da informação, falando dos serviços a serem instalados em um ambiente fictício e configurações a serem feitas para diminuir os riscos.

SUMÁRIO

1 INTRODUÇÃO

O ambiente pensado para a instalação dos serviços será uma pequena empresa, neste ambiente será instalado serviços cruciais para o funcionamento da mesma, em que os produtos são apresentados por meio do site, as vendas são feitas por telefone e os documentos sempre enviados via e-mail para a concretização da venda e manter os registros dos mesmos.

2 SISTEMA OPERACIONAL

O Sistema Operacional que iremos usar é o CentOS 7, instalado na versão miníma para uma melhor administração já que por padrão apenas o necessário é instalado inicialmente. Todas as instalações passaram pelo processo de *Hardening* para que nenhuma brecha conhecida possa ser explorada por pessoas mal intencionadas, o sistema será atualizado periodicamente, primeiramente em ambiente de teste e se não acontecer nenhum conflito entre os serviços será reproduzido em ambiente de produção.

3 SERVIÇOS

Os serviços que serão instalados são HTTP, SMTP, SSH e DHCP. Em HTTP irá ser usado o programa APACHE.

3.1 HTTP

Ao instalar o APACHE algumas configurações de segurança devem ser feitas para mitigar as vulnerabilidades entre elas estão:

- Manter o APACHE atualizado com as últimas versões e correções;
- Desativar a lista de diretórios;
- Desativar módulos desnecessários;
- Desativar os serviços desnecessários;
- Certificar de que o serviço “Server-Info” esteja desabilitado;
- Desativar o rastreamento HTTP Request;

- Não executar o APACHE como root;

3.2 SSH

O SSH vai ser usado para que o Help Desk acesse os computadores e agilize o suporte aos usuários no caso de algum problema. Será instalado em todas as maquinas que receberam acesso de suporte inclusive o servidor e receberá configurações de segurança para garantir que apenas as pessoas autorizadas tenham acesso, entre elas:

- Alteração da porta padrão;
- Desabilitar login do root;
- Diminuir o tempo para digitar a senha;
- Diminuir o tempo de inatividade;
- Permitir usuários específicos;

3.3 HTTP

O servidor que irá transmitir os endereço de IP será configurado o DHCP e receberá configurações para garantir que nenhuma máquina não autorizada receba um endereço e tenha acesso a rede tanto cabeada quanto wireless.

- Verificar que pessoas não autorizadas tenham acesso a rede;
- Habilitar log;
- Monitorar constantemente a rede;
- Vincular endereço de IP ao MAC de máquinas autorizadas;

3.4 SMTP

o SMTP é o protocolo responsável por transferências de mensagens de e-mail. Em nossa empresa o e-mail é de suma importância para o fechamento das vendas e envio de nota fiscal e para que saia errado ou que mensagens desnecessárias sejam recebidas medidas de segurança devem ser tomadas, abaixo algumas delas;

- Mudando a porta para 587, conforme Decreto nº 4.829/2003 do CGI;
- Habilitar autenticação de envio de mensagens;
- Utilização do protocolo SSMTP;
- Medidas anti-spam;
- Orientação dos usuários sobre a utilização do e-mail;

4 BIBLIOGRAFIA

- www.imasters.com.br;
- www.vivaolinux.com.br;