cespe

Cebraspe
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos

CONCURSO PÚBLICO – TRE/RS

CARGO 2: ANALISTA JUDICIÁRIO
ÁREA: APOIO ESPECIALIZADO
ESPECIALIDADE: ANÁLISE DE SISTEMAS

Prova Escrita – Questão 2

Aplicação: 20/12/2015

PADRÃO DE RESPOSTA

1 Duas soluções técnicas que abranjam o uso de ferramentas ou de configurações protetivas para a infraestrutura computacional do órgão e as funcionalidades aplicáveis efetivamente úteis no combate aos *emails* de *phishing*

Instalar junto aos servidores de *email* ferramentas e soluções *antispam* com funcionalidades *antimalware*; de verificação de idoneidade e reputação de domínios, de filtragem de mensagens comerciais indesejadas (*spam*), mensagens com conteúdo falso, mensagens com origens falsificadas ou reconhecidas como maliciosas; bloqueio e remoção de anexos maliciosos, links maliciosos; bloqueio de saída para sítios de *phishing* e distribuidores de *malware*; interação com bases de dados de empresas especializadas em fraudes e *malware*, bem como instalar e manter atualizados sistemas de segurança como programas *antimalware*, *antispam* e *antiphishing* nas estações de trabalho dos colaboradores.

Realizar configurações para manter *relay* fechado por *default*, permitir *relay* autenticado, estabelecer *relay* incondicional restrito a rede local; bloquear mensagens oriundas de endereços IP inválidos ou reconhecidos como veiculadores de mensagens maliciosas, mensagens oriundas de domínios inválidos, inexistentes, inconsistentes ou reconhecidos como proliferadores de *spam* e *phishing*; configurar *blacklists* e *graylists*; configurar regras de verificação de consistência do DNS reverso e das *strings* do DNS reverso, regras de verificação de consistência do comando `MAIL FROM`; verificar *null-reverse path*, uso do domínio local, “caracteres proibidos” e capacidade do servidor remoto para receber conexões SMTP.

2 Cinco recomendações práticas e de caráter educativo aos colaboradores do órgão, com objetivo específico de combater a prática de *phishing* e abusos no uso de *email*

Desconfie, não responda e apague mensagens que ofereçam vantagens inesperadas e ofertas imperdíveis, que requeiram que o usuário clique em *link* ou em anexos; que solicitem antecipação de recursos em prol de benefício futuro; que imponham situações de pressão, ameaça ou dificuldades como dívidas, intimações, protestos, vexames; que proponham benefícios emocionais ou sexuais; que venham de origens desconhecidas; que solicitem informações pessoais e de cadastro; que requeiram ações não padronizadas em relação ao ambiente de rede da organização.

Não informe seu endereço do *email* corporativo em formulários de cadastro de sítios comerciais, em fóruns e listas de discussão, em comentários de sítios de notícias e redes sociais; se for realmente necessário, crie e use contas de serviços de *email* públicos.

Não repasse mensagens com notícias, informações, pedidos de ajuda, utilidade pública, alertas, apelos, acusações, correntes ou propagandas, vindas de quaisquer origens, sem a devida comprovação de veracidade junto à suposta fonte original.

Notifique à área de segurança em TI eventuais incidentes e abusos relacionados ao uso de *email* como *phishing*, *spam*, boatos, correntes, *links* suspeitos e anexos maliciosos.

Mantenha seus sistemas de segurança de *email* da estação de trabalho atualizados e ativos.