[IMPORTANTE] DETEC/CITEM - Falsificação de e-mail/Tentativa indevida de coleta de informações

Comunicação DETEC/CITEM
Qua, 30/10/2019 15:53

GOVERNO DO ESTADO DE SÃO PAULO

Secretaria da Educação do Estado de São Paulo
Coordenadoria de Informação, Tecnologia, Evidência e Matrícula

DETEC – Departamento de Tecnologia de Sistemas
CEIR – Centro de Infraestruturas de Rede
CIEQ – Centro de Instalações e Equipamentos
CPLIS – Centro de Planejamento e Integração de Sistemas

30/10/2019 Departamento de Tecnologia de Sistemas – DETEC
Falsificação de e-mail/Tentativa indevida de coleta de informações

Prezado(a)s,

A CITEM/DETEC informa que há uma tentativa de obter informações e instalar códigos maliciosos através de e-mail solicitando que **"todos os clientes atualizem suas informações para evitar o encerramento ou suspensão de contas de e-mail"** e ainda **"uma tentativa incorreta de senha desabilita sua conta"**.

Pedimos a todos que o e-mail malicioso seja excluído, não devendo o usuário clicar no link ou compartilhar seu conteúdo.

É importante lembrar que o sucesso da Segurança da Informação depende de todos os servidores, e não só da equipe técnica de TI ou das ferramentas utilizadas para evitar falhas ou ataques maliciosos.

É dever de cada servidor zelar pela preservação das informações de seu órgão, pois atualmente elas são um dos mais importantes ativos do estado e possuem características e restrições distintas.

Grande parte dos ataques atuais busca alguma falha, quer de ordem técnica ou comportamental. Simples e-mails, contendo anexos ou links maliciosos, podem ser uma ameaça que causará um enorme prejuízo para as instituições.

Em complemento, encaminhamos algumas dicas de segurança adicionais, afim de ajudar a prevenir essas ameaças:

1. Backup

Os servidores devem salvar seus documentos ou informações de trabalho em Pastas na Rede Local e/ou serviços de nuvem institucionais, de preferência com backups diários.

É sempre um risco manter as informações apenas nas estações de trabalho e sem backup, pois problemas podem ocorrer, não só causados por estas ameaças, como também por razões técnicas – por exemplo, um HD defeituoso.

2. Uso do e-mail

O servidor sempre deve estar atento a e-mails de pessoas desconhecidas, evitando clicar em anexos de origem duvidosa. Isso é de vital importância, pois uma das principais técnicas de ataque dos hackers continua sendo o envio de e-mails contendo links e/ou anexos maliciosos que, caso acessados, podem provocar vários tipos de danos, dos computadores à própria rede como um todo.

3. Navegação

Ao navegar na internet, o servidor deve evitar acessar sites de conteúdo suspeito ou não autorizados. Nunca baixe qualquer arquivo, de qualquer tipo, de fontes desconhecidas. Da mesma forma, é necessário extremo cuidado com anexos e links recebidos nas redes sociais.

4. Estação de Trabalho (Computador)

Alterações nas configurações do sistema operacional, de rede e de outros programas só são realizadas pelo suporte técnico de sua localidade, e com prévia autorização da chefia imediata, se for o caso.

O procedimento é o mesmo para a instalação de novos softwares.

5. Dispositivos de armazenagem externa

O servidor deve agir com cautela na utilização de dispositivos de armazenagem externa, como pendrives e HDs Externos, pois eles podem conter e-mails de origens duvidosas e até mesmo malwares que podem ser transferidos para a máquina ou para a rede local.

6. Contribua com a segurança

Todo servidor é parte fundamental deste processo de prevenção!

Além dos cuidados básicos aqui listados, é de suma importância que quaisquer situações ou comportamentos que tragam risco para a instituição sejam relatados pelos servidores ao suporte técnico de sua localidade.

A Secretaria da Educação, através do seu Departamento de Tecnologia de Sistemas e Inclusão Digital, em conjunto com a Fundação para o Desenvolvimento da Educação, monitora constantemente toda a rede, certificando-se que sempre serão aplicadas as melhores práticas em todo seu parque tecnológico.

Caso tenha curiosidade sobre esse tipo de assunto, recomendamos a leitura do Manual do Comitê Gestor da Internet no Brasil http://internetsegura.fde.sp.gov.br/Arquivos/cartilha-seguranca-internet.pdf.

Contamos com a colaboração de todos.

Atenciosamente.

DETEC - Departamento de Tecnologia de Sistemas
CITEM - Coordenadoria de Informação, Tecnologia, Evidencia e Matrícula.