GOVERNO DO ESTADO DE SÃO PAULO

Secretaria da Educação do Estado de São Paulo

Coordenadoria de Informação, Monitoramento e Avaliação Educacional

DETEC - Departamento de Tecnologia de Sistemas e Inclusão Digital

CEDIG - Centro de Inclusão Digital

CIEQ – Centro de Instalações e Equipamentos

CPLIS – Centro de Planejamento e Integração de Sistemas

17/05/2017 - Departamento de Tecnologia de Sistemas e Inclusão Digital – DETEC

Prevenção contra Ciberataques

A última sexta-feira, dia 12 de maio, ficou marcada por um grande ataque mundial que afetou mais de 200 mil computadores em cerca de 150 países. Notícias e relatórios apontam que organizações públicas e privadas ao redor do mundo foram impactadas, uma vez que tiveram que parar suas produções, fábricas ou serviços.

O culpado é o ransomware “WannaCrypt”, que utilizou uma vulnerabilidade nos sistemas Microsoft Windows para infectar as máquinas.

Ransomware é um código malicioso que infecta computadores com o objetivo de sequestrar, capturar ou limitar o acesso a dados ou informações de um sistema, geralmente por meio do uso de algoritmos de encriptação, para fins de extorsão. Para obter a chave de decriptação, geralmente é exigido um pagamento (Ransom) usando-se moedas virtuais, tipo “Bitcoins”. A transmissão do Ransomware é realizada via e-mails maliciosos (spam) e arquivos infectados disponibilizados para download.

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.

Cabe salientar que, no mesmo dia em que os ataques foram noticiados, a Fundação para o Desenvolvimento da Educação – FDE, responsável técnica pela gestão da segurança de nossa rede, encaminhou comunicado discorrendo sobre a questão, reiterando aos usuários alguns cuidados básicos na utilização dos recursos de rede e internet.

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 e Inclusão Digital
CIMA - Coordenadoria de Informação, Monitoramento e Avaliação Educacional