TRIBUNAL DE CONTAS DO ESTADO DE SÃO PAULO
Av. Rangel Pestana, 315 – Centro - CEP 01017-906 - São Paulo/SP-PABX: 3292-3336
Coordenadoria de Comunicação Social (CCS) – Jornalista responsável: Laércio Bispo MTB 33.444

RELEASE
11/11/2020

Segurança Digital: responsabilidade de todos

***Fabio Correa Xavier**

Diretor do Departamento de Tecnologia da Informação do Tribunal de Contas do Estado de São Paulo (TCESP)

Confidencialidade. Integridade. Disponibilidade. Esses são pilares que a segurança da informação deve manter em relação aos dados, aos sistemas e à infraestrutura tecnológica. Confidencialidade é garantir que a informação estará disponível somente para quem dela deve fazer uso. Integridade, por sua vez, é garantir que a informação seja exata, completa e que não foi alterada indevidamente. E disponibilidade, por fim, é garantir que a informação esteja disponível sempre que for necessária. Porém, é importante destacar que, como em qualquer outra área, há três aspectos que devem ser considerados para uma segurança da informação eficiente: a tecnologia, os processos e o fator humano.

Historicamente, a segurança da informação tem sido vista como uma responsabilidade exclusiva da área de tecnologia da informação das organizações. Esse é um erro comum que causa muitos problemas, pois essa área pode lidar muito bem com os aspectos tecnológicos (*softwares* e *hardwares* de proteção, como *firewalls* e antivírus), com a implantação de estratégias de prevenção em várias camadas e com mecanismos de detecção e de resposta integrados. Pode, ainda, lidar com os aspectos de processos, criando procedimentos e regras – claro que esses procedimentos e regras devem ser aprovados pela alta administração das organizações.

Contudo, o aspecto humano nem sempre é devidamente considerado na segurança da informação. E os fraudadores sabem e exploram isso ao máximo. Segundo dados coletados pela empresa de segurança da informação Fortinet, somente em março deste ano surgiram 600 novas campanhas de *phishing* por dia. O relatório 'The Fraud Beat' da Cyxtera, outra empresa especializada em segurança da informação, demonstra que 90% dos ataques começam com o *phishing*. E o que é o *phishing*? Pode ser exemplificado por aquele *e-mail* que recebemos, pedindo para informarmos dados como nome, CPF, endereço eletrônico e senhas. Assim, os fraudadores

conseguem acesso aos sistemas e às redes com credenciais válidas, que foram roubadas dessa forma. E os fraudadores estão aprimorando cada vez mais esses *e-mails* 'isca'. Eles utilizam mensagens parecidas com um *e-mail* válido e assuntos e temas relevantes para a organização que está sendo alvo do ataque. Recentemente, no Tribunal de Contas do Estado de São Paulo (TCESP), recebemos *e-mails* falsos sobre folha de pagamento e um supostamente da Caixa de Assistência dos Advogados de São Paulo (CAASP), que continham *links* para *sites* ilegítimos, praticamente idênticos aos reais. Essa técnica de fraude não se restringe a *e-mails*: também podem ser utilizadas outras formas de comunicação como o 'WhatsApp', SMS e redes sociais.

Nos últimos dias, foram veiculadas notícias sobre ataques ao Superior Tribunal de Justiça, ao Ministério da Saúde e ao Governo do Distrito Federal. Provavelmente, esses ataques tiveram origem em um phishing bem-sucedido, que obteve credenciais de acesso à rede e, uma vez dentro, o hacker usou técnicas para aumentar o seu nível de privilégio e usar um ransomware, que é um software que restringe o acesso aos dados e às máquinas virtuais, criptografando tais informações. A liberação do acesso se dá, geralmente, por meio de pagamento de um 'resgate' em bitcoins, uma criptomoeda que garante transações anônimas.

Mas como podemos evitar que isso ocorra? A tecnologia, certamente, é importante. Mas tão importante quanto ela é a conscientização de que a segurança depende de todos. Um comportamento digital seguro é parte fundamental da segurança da informação. E, para isso, listo algumas recomendações importantes:

- Nunca clique em *links* de *e-mails* suspeitos. Desconfie sempre.
- Nunca, nunca mesmo, coloque sua senha em formulários, em resposta a *e-mails* ou passe por telefone. Ela só deve ser digitada para acesso aos sistemas e *e-mails*. Se alguém pedir sua senha, certamente não é bem-intencionado.
- Use senhas com caracteres maiúsculos, minúsculos, números e caracteres especiais. Quanto maior e mais diversificada for a senha, melhor. E, importante: troque-a regularmente.
- Não use suas credenciais profissionais para fins particulares, como cadastro em listas de discussão, fórum, sites de compras e redes sociais, dentre outros.

- Mantenha seu equipamento com *firewall* pessoal e antivírus atualizado.
- Fique atento aos comunicados da área de segurança da informação do Departamento de Tecnologia da Informação e, em caso de dúvidas, entre em contato.

Lembre-se: a segurança digital é responsabilidade de todos e, principalmente, de cada um de nós.