IDG NOW! tecnologia em primeiro lugar http://www.idgnow.com.br

COMPUTAÇÃO CORPORATIVA >

4 hábitos que fazem dos executivos alvos prediletos de golpes na Internet

(http://idgnow.uol.com.br/computacao_corporativa/2010/07/14/4-habitos-que-fazem-dos-executivos-alvos-prediletos-de-golpes-na-internet)

Por CSO / EUA

Publicada em 15 de julho de 2010 às 08h35

Desatentos para questões de segurança e convictos de estarem protegidos, eles são os primeiros a passar por cima das normas elaboradas pela TI.

Os responsáveis pela gestão da segurança da TI são os primeiros a ficarem preocupados com o uso de redes sociais por funcionários capazes de cair no conto de alguém que se diz em apuros em uma localidade distante - os velhos golpes do tipo 419.

Outros se preocupam com aqueles funcionários que acreditarão estar falando com um príncipe nigeriano querendo dividir uma fortuna.

E há mais uma fonte de preocupação: as mensagens disfarçadas de e-mail de bancos. Esses golpes virtuais são a motivação que faltava para a empresa dar início a um programa de conscientização do perigo que essas ações trazem.

Mas, de acordo com o consultor de segurança e CIO da empresa Stratagem 1 Solutions, Jayson Street, o cerne da preocupação não deveria ter como foco os funcionários em geral e sim os executivos de alto poder de decisão dentro da organização. Se alguém precisa de instruções sobre como lidar com essa questão, são eles.

Street realiza estudos de penetração desses golpes e fornece treinamento para corrigir “os bugs humanos”. Ele aponta para os executivos com acesso a informações confidenciais como alvos prediletos na hora desses golpes.

Eles estão em condições de comprometer seriamente a organização. A ameaça somente poderá ser considerada sanada quando o termo “segurança” for largamente disseminado dentro da empresa, do nível mais baixo até o mais alto.

“Precisamos de executivos atentos aos perigos”, afirma. “Ao saberem o que lhes pode acontecer, estarão aptos a evitar os riscos.”

Seguem os quatro motivos que incentivam os golpistas a mirar nas caixas de entrada desses profissionais para aplicar os golpes.

1::Sentem-se acima das regras de segurança
Street afirma que, por serem as pessoas mais importantes dentro das empresas, os executivos têm atribuições que lhes tomam muito tempo. Isso lhes da a sensação de não estarem sujeitos a seguir a cartilha de politicas de segurança.

“Eles acham que o firewall serve para os outros, e que os bloqueios não devem ser aplicados em suas estações de trabalho”, explica. “Os executivos não querem ter o tráfego de suas máquinas filtrado, rastreado ou monitorado. Dessa maneira, saem da rota dos proxies, a única proteção com a qual contavam.”

O fato é que esses executivos não são muito mais espertos quando o assunto é segurança, quando comparados aos funcionários “rasos”. E, pelo fato de serem executivos, o golpe é normalmente muito mais refinado e pessoal, dando a impressão de ser alguma mensagem oriunda de um remetente legítimo, apesar do anexo ser um arquivo danoso.

2::Acham que a TI dá conta de tudo
“Depois que um executivo executa o arquivo anexo e tem a máquina infectada, é certo que vai se virar para o departamento de TI e indagar por que ninguém cuidou da segurança”, diz Street.

Recentemente Street concluiu uma série de ensaios de penetração a mando de dois hotéis, obteve acesso aos servidores e enviou mensagens falsas fazendo-se passar pelo CEO da empresa responsável pelo suporte técnico do hotel.

“Depois, perguntei por que motivo me haviam deixado entrar. A resposta era que o dono do hotel fazia isso o tempo todo. Que o proprietário passava e-mails desse tipo o tempo todo.”

A questão que se apresenta é: o executivo, nesse caso o proprietário do hotel, não compreende que, ao agir dessa maneira (não tendo um sistema que verifique o remetente de mensagens eletrônicas), expõe toda a organização a um risco desnecessário, confiante de estar coberto pelo TI no caso de lago dar errado.

3::Tecnologia de ponta resolve qualquer problema
“Os CIOs são um alvo querido por golpistas por usarem sempre recursos modernos de segurança”, afirma Street.

“Quem, dentro da empresa, vai ter permissão de usar o iPhone mais recente ou poderá ter um iPad conectado à rede interna para receber e-mails?”, Street pergunta. E responde: os altos executivos. “Eles compram notebooks com sistemas não homologados, querem o laptop ultrafino e leve, capaz de executar determinadas tarefas”, diz.

O problema é que esses dispositivos não passaram pelo crivo do TI nem foram configurados para acessar a rede de maneira segura. Frequentemente também têm a impressão de o departamento de TI já estar apto a lidar com as falhas intrínsecas às novas tecnologias – é onde se enganam.

“Os executivos partem dos princípio de que “mais moderno” significa “mais seguro”, um ledo engano. Mesmo assim, insistem em conectar-se à rede em suas residências, e acabam confundindo os dois ambientes”, pontua Street.

4::A família ignora os riscos
“O golpista sempre irá procurar por uma maneira mais fácil de chegar até o executivo. Como o departamento de TI pode estar atento às mensagens da caixa de entrada do CIO, é mais fácil ir atrás da esposa e dos filhos nas redes sociais, como o Facebook”, afirma Street. É comum o executivo compartilhar seu computador com o resto da família.

“Por que não infectar o computador da esposa e esperar que o executivo se conecte na mesma rede? O ambiente de rede doméstico é mais confiável que o corporativo e o firewall certamente está configurado para manter regras mais frouxas de bloqueio de tráfego. É a maneira mais prática de chegar ao executivo ”, ressalta.

Segundo o analista, estar atento para o perigo desses golpes é importante, inclusive, para os membros da família – alvos fáceis para as ações criminosas. “Quando se trata de milhões de dólares e há a intenção de roubar segredos corporativos, ou de espionar as ações de concorrentes, o mais fácil é incluir todo mundo que está na rede de contatos do executivo-alvo”, finaliza Street.

(Joan Goodchild)