CRÓNICA VISÃO ELECTRÓNICA
Nº 049 / 2009-12-23
http://www.gestaodefraude.eu

Edgar Pimenta

> > Sistemas de informação: Redutores ou impulsionadores da fraude?

1. Existem várias teorias que tentam explicar as razões que conduzem a um acto criminoso. Até inícios do século XX, uma das principais teorias defendia a tendência genética para a criminalidade. Era uma teoria baseada na observação do crime comum. Nos anos trinta, Edwin Sutherland (o pai dos termo "crime de colarinho branco") desenvolve a teoria de associação diferencial. Sucintamente, defendia que o crime se aprende e que o contexto sócio-cultural do indivíduo tem influência decisiva.

Nos anos 40, Donald R. Cressey (aluno de Sutherland) foca os seus estudos numa classe particular de criminosos, os defraudadores (designados como "violadores de confiança"). É nesse âmbito, e após entrevistar 200 detidos em várias prisões, que formula a seguinte hipótese associada à fraude ocupacional: "*as pessoas, em quem se confia, tornam-se violadoras dessa confiança quando imaginam que têm um problema financeiro impossível de partilhar e que acreditam poder ser secretamente resolvido, através da violação da confiança financeira, sendo capazes de aplicar à sua conduta, naquela situação, justificações que lhes permitam ajustar o conceito, que têm de si próprios, de pessoas de confiança de utilizadores dos fundos ou propriedade que lhes foram confiados*". Esta hipótese acabou por ganhar notoriedade através do que é chamado o Triangulo da Fraude.

Pressão, oportunidade e justificação são os vértices deste triângulo. A pressão resulta da existência de uma necessidade financeira não partilhável, a oportunidade apercebida de resolver essa necessidade financeira e a justificação, que nada é mais do que um processo de racionalização que ajuda à neutralização de padrões éticos ("toda a gente o faz", "já que a empresa não reconhece o meu mérito"). Ainda segundo Cressey, o defraudador teria que ter informação geral e conhecimentos de como realizar a fraude com sucesso.

Embora tenham surgido novas teorias para explicar as razões que conduzem à perpetração da fraude, o triangulo da fraude é ainda uma base e umas das teorias mais comummente usadas.

CRÓNICA VISÃO ELECTRÓNICA
Nº 049 / 2009-12-23
http://www.gestaodefraude.eu
Edgar Pimenta

Mas será que as evoluções tecnológicas dos últimos anos, a dependência cada vez maior das organizações e o surgimento de novos tipos de fraude com recurso à informática veio alterar este panorama?

2. Olhemos os sistemas de informação na perspectiva da prevenção e detecção da fraude ocupacional. No lado da prevenção, a implementação de controlos com base nos sistemas de informação permite automatizar actividades de controlo que anteriormente seriam, eventualmente, feitas de forma manual. Simultaneamente, torna-se muito mais simples implementar novos controlos, diminuindo claramente as oportunidades de fraude ocupacional.

Do lado da detecção, é inevitável referir as ferramentas de *data mining*. Estas ferramentas, graças à sua capacidade de tratamento de volumes de informação massivos, permitem encontrar informação e conhecimento em dados aparentemente desinteressantes. Permite-nos ainda correlacionar informação, analisar padrões e detectar os famosos *outlier* (valores estatisticamente distintos do resto da informação). De facto, os sistemas de informação permitem actualmente análises, desde as mais simples às mais complexas, análises estas que podem ser primeiros indícios de fraude.

Aparentemente, poderíamos ser levados a considerar que os sistemas de informação e as novas tecnologias permitiriam um maior controlo sobre as situações de fraude ocupacional. Mas será?

3. As organizações estão cada vez mais reféns da tecnologia, da informática. A informação detida pelas organizações é cada vez mais valiosa, mas simultaneamente guardada num meio, eventualmente, mais volátil: o meio digital. E até há relativamente pouco tempo, este era considerado um meio seguro. Uma organização, a partir do momento em que se informatizava, via todos os seus problemas resolvidos. Felizmente, essa mentalidade tem vindo a mudar. E ainda bem. Porque os sistemas de informação, se por um lado vieram ajudar na detecção e prevenção da fraude, também vieram abrir novos desafios, novas necessidades.

Os sistemas de informação não são inerentemente seguros.

CRÓNICA VISÃO ELECTRÓNICA
Nº 049 / 2009-12-23
http://www.gestaodefraude.eu

Edgar Pimenta

Não existe segurança "out of the box". Todos os sistemas devem ser alterados, costumizados de forma a fornecer um nível de segurança adequado e permitir simultaneamente a fácil usabilidade do sistema. Este é o primeiro desafio. O desafio seguinte consiste em manter o sistema. Todos os sistemas têm falhas, bugs, vulnerabilidades. É necessário mantê-los actualizados. Caso contrário, alguém mal intencionado poderá utilizar essas vulnerabilidades como ponto de partida para algum tipo de fraude. E este é um dos grandes problemas nos tempos actuais, sobretudo por duas razões: a típica negligência a proteger os sistemas dos utilizadores internos e a proliferação do crime organizado.

Quando se fala em segurança dos sistemas de informação, tipicamente, a primeira preocupação é garantir que os sistemas de informação estão devidamente protegidos do exterior. Esta preocupação é obviamente válida, mas o erro está em normalmente ficarmo-nos por aí. Devemos olhar para dentro das organizações e proteger igualmente o acesso á informação a partir dos "insiders". Mas desengane-se quem pensa que essa protecção se baseia em atribuir nomes de utilizadores e palavras-passe para acesso aos sistemas. Esse é um passo, mas apenas o primeiro de muitos. Atribuição de acesso apenas à informação necessária para a execução das suas funções, ajustamento dos acessos na sequência de alterações funcionais (dos colaboradores ou da própria estrutura orgânica da organização), são apenas alguns passos. Muitos outros existem. Uma das principais alterações necessárias, e talvez a mais difícil, é a mudança cultural. É embutir dentro de cada um de nós uma cultura de segurança. É deixarmos de emprestar o nosso nome de utilizador a um colega de trabalho que até é "porreiro", deixamos de escrever as palavras-passe num post-it que colocamos no monitor ou, para ser muito mais seguro, debaixo do teclado. É sermos mais sensíveis para as questões da segurança da informação.

O crime informático é cada vez mais uma actividade organizada, onde o lado infractor dispõe de elevados recursos financeiros e técnicos. E o critério de escolha do alvo deixa der ser aquele que aparenta maior fragilidade no sistema para passar a ser aquele que mais lucro pode render. E definido o alvo, é necessário apenas ver o melhor método. E um dos que será garan-

tidamente considerado é a utilização de conhecimento interno à organização através dos seus colaboradores. E estes podem participar ou de forma voluntaria, ou sob coação, ou através de dissimulação. E se a organização não se protegeu devidamente contra ataques internos? E se cada colaborador da organização fosse um potencial hacker? Ok... estamos num nível de paranóia elevado. Isso não acontece na minha organização poderá estar o leitor a pensar. Não acontece? Ou acontece mas simplesmente não sabe?

Ou seja, a tecnologia, a informática, os sistemas de informação, se por um lado vieram ajudar ao controlo de actividades que potencialmente podem ser consideradas como indícios de fraude, simultaneamente, vieram criar novos desafios para garantir que essas mesmas fraudes não ocorram.

Estaremos nós a enfrentar correctamente estes novos desafios?