ANTÓNIO ROLHAS

TEMAS DE FRAUDE EM TELECOMUNICAÇÕES — PARA UMA CULTURA DE SEGURANÇA

Embora exista uma panóplia de definições de fraude em telecomunicações, há, no entanto, um consenso generalizado de que a fraude nesta temática envolve o furto ou o abuso deliberado da utilização de serviços prestados pelos operadores e prestadores de serviços. A intenção do autor da fraude é evitar completamente ou, pelo menos, reduzir os custos associados à utilização de serviços que são normalmente cobrados. Em suma, a fraude envolve um qualquer esquema criado com má fé para obter ganhos de forma ilícita, implicando a consequente perda de proveitos por parte de terceiros.

Do mesmo modo que existem várias definições de fraude também há diferentes métodos de a cometer. Aqui, na área das telecomunicações, a fraude está associada à forma como é cometida e às motivações por detrás da sua realização: entretenimento ou satisfação intelectual, prazer de «conseguir», vingança, desconhecimento de que se está a fazer algo que é proibido ou ilícito e, sobretudo, intuito lucrativo. Este último está normalmente associado a complexos esquemas e a organizações interligados com o crime organizado, tráfico de estupefacientes, armas, prostituição, branqueamento de capitais, entre outros.

A fraude em telecomunicações tornou-se numa indústria com relações a nível internacional e mesmo intercontinental. A tecnologia permite comunicações céleres, permitindo redes de contacto extremamente organizadas, que vão desde o âmbito local até ao internacional. Tratando-se de redes organizadas e com sistemas de financiamento robustos, possuem ainda acesso à tecnologia mais sofisticada, seja em termos de equipamentos como de serviços. De igual modo, têm também acesso aos mais sofisticados métodos de acesso, legais ou ilegais, o que torna a aquisição, importação ou absorção de conhecimento imediata.

Contudo, a principal razão por que os autores de fraude cometem esse acesso ilegal, ludibriando todo um mercado de telecomunicações, é porque lhes é permitido fazê-lo. Quem decide criar um esquema (ilícito) de fraude, também o termina logo que entende fazê-lo. Ou seja, trata-se de uma atividade contínua que, quando tiver de ser interrompida, poderá sê-lo de um momento para o outro. O autor de fraude tem conhecimento do que quer fazer e sabe os riscos que corre ao ser «apanhado». Em todo o caso, quanto maior for a dificuldade de cometer fraude e quanto maior for a perceção de efetiva deteção e punição, menor é o potencial da fraude ocorrer. O autor da fraude procede a uma avaliação da recompensa e do risco associado e, se a recompensa não compensar o risco, a probabilidade de ocorrer a fraude será naturalmente menor.

Nestes últimos anos de desenvolvimento das telecomunicações no nosso país, não tem havido uma cultura de segurança. Havia alguém que dizia, com as devidas adaptações, que há dois tipos de entidades: as que já foram alvo de fraude e aquelas que não sabem que foram alvo de fraude. O combate à fraude tem acompanhado o desenvolvimento das telecomunicações e da tecnologia. Normalmente, nas empresas de telecomunicações, existem por lá «um ou dois tipos», encaixados numa qualquer caixa de um organigrama, que se preocupam com este tipo de assuntos. Pessoas esquisitas...

Mas quando se fala nas empresas, as tais que prestam os serviços, temos de falar também nas autoridades policiais e reguladoras. A fraude não pode ser considerada ficção científica como sucede na mente de alguns. Ela está presente no dia a dia. E quando ela acontece e é notícia de primeira página, a pirâmide organizativa vem por aí abaixo para saber quem é que detém o conhecimento ou o contato certo para resolver o problema. Só quando o assunto é sério e passível de envolver a dinâmica de um país é que os responsáveis das organizações começam a ficar sensibilizados para o tema. Por vezes, é difícil convencer os responsáveis das empresas e autoridades públicas a investirem no combate e prevenção da fraude. No entanto, trata-se de uma prioridade e de uma preocupação que não podem ser subestimadas face a outras prioridades das organizações e do próprio Estado.

Os intervenientes no mercado de telecomunicações não podem viver de costas voltadas uns para os outros. Têm de cooperar. A experiência diz-me que cooperam. Apesar do mercado ser liberalizado e estar em concorrência, e para além da defesa dos seus negócios, o combate à fraude é realizado, hoje em dia, por um núcleo reduzido de pessoas, que se conhece, que troca informação importante acerca de novas metodologias de fraude e que se empenham mutuamente nessa luta em prol do desenvolvimento das telecomunicações no país.

Os perfis típicos da fraude em telecomunicações são tipificados, sinalizados, organizados, catalogados, combatidos e eliminados de modo a que a prestação dos serviços continue a decorrer. Por vezes, não existe a perceção imediata desses perfis, que podem sofrer alterações com o decorrer do tempo, pelo que uma monitorização diária e permanente revela-se numa tarefa deveras importante, ainda que demasiado complexa.

Para um prestador de serviço, a análise isolada de um evento de fraude é uma operação relativamente simples. A maior dificuldade é distingui-la de entre milhares de eventos, milhões de registos, milhares de alterações do perfil de consumo, centenas de novos clientes e diferentes fontes de informação, entre outros fatores. O cruzamento de todas estas variáveis de eventos torna a gestão da fraude quase impossível sem o recurso a processos automáticos de computação. No entanto, mesmo recorrendo a esses poderosos sistemas automáticos, é indispensável a seleção e segmentação da informação mais relevante. Não é financeiramente interessante gastar, por exemplo, milhares de euros para impedir fraudes de € 50. No entanto, o que está por detrás desses € 50 é informação que, utilizada de modo correto, poderá impedir eventos futuros de fraude que poderão causar prejuízos de milhões.

O processo de gestão da fraude em telecomunicações envolve três atividades distintas, mas interdependentes: prevenção, deteção e investigação. Cada uma das entidades competentes no combate à fraude efetua uma avaliação de cada uma daquelas vertentes e equaciona a melhor forma de abordagem em conjunto.

O sucesso deste processo, ou a estratégia de atuação, tem de ter a concordância dos seus responsáveis para que a mesma seja bem-sucedida.

Considere-se, hipoteticamente, que uma empresa prestadora de serviços é alvo de perdas por fraude de subscrição. Para determinar que essas perdas são reais e distingui-las dos incumprimentos normais, é necessário um processo, manual ou automatizado, para detetar casos de possíveis fraudes. Esse processo de deteção fornecerá uma base para investigação sobre como as perdas ocorreram e, já agora, quão exposta a empresa está a novos esquemas de fraude. Os resultados da investigação irão desencadear ações destinadas a evitar perdas futuras, e estas, por sua vez, resultarão em revisões do processo de deteção, realimentando todo o processo de combate à fraude, em antecipação a novos estratagemas por parte dos autores de fraude.

Não existe um guia ou um manual que instrua sobre como realizar uma fraude. Como são várias as categorias de fraude, mais ou menos conhecidas, são disponibilizados «tutoriais» em vídeo nas redes sociais, que explicam desde a fraude mais simples à mais sofisticada. Por outro lado, também não existe um guia de combate à fraude. Existe sim o conhecimento e a troca de informação entre pessoas, o tal núcleo reduzido, numa relação de confiança que se constrói com o tempo.

A fraude móvel — sendo a mais conhecida a clonagem — é uma fraude técnica com um «sabor a James Bond», que conquistou a imaginação dos jornalistas de tecnologias de informação e comunicação.

A segurança tecnológica tornou-se robusta, pelo que os agentes de fraude começaram a rumar para outras áreas de usufruto de serviços sem intenção de pagar. Desde clientes falsos ou assinaturas forjadas para passar nos processos de classificação e obtenção de serviço, tudo vale(u). A obtenção de serviços de telecomunicações com uma assinatura falsa pode permitir o maior número possível de chamadas telefónicas, por exemplo, chamadas internacionais ou mesmo intercontinentais, de alto custo, antes de o serviço ser desligado por falta de pagamento. Se a situação ocorrer em *roaming* internacional tanto melhor. Aqui, o autor da fraude vai para outro país, efetua chamadas telefónicas sabendo que o seu prestador local demora mais tempo a receber e a processar os registos de *roaming* do que o necessário do que habitualmente necessita para processar as chamadas efetuadas dentro da rede. Foram vários os casos que aconteceram ao longo do tempo. Como é evidente, tratando-se de assuntos de natureza reservada ao negócio do prestador de serviços, tais casos não são publicitados.

A rede fixa sofreu, ao longo do tempo, esquemas diversos de fraude. Foram até em maior número do que os perpetrados na rede móvel, cujo desenvolvimento da tecnologia é mais recente, logo, com métodos de combate mais sofisticados. Uma das fraudes mais utilizadas era a que dizia respeito aos sistemas telefónicos das empresas. Numa análise mais profunda às faturas do consumo telefónico poderiam detetar-se esquemas ou eventos de fraude. Porém, a inexistência de uma cultura de segurança ou combate à fraude não permitia a deteção deste tipo de esquemas. Só quando a conta telefónica surgia exageradamente alta é que o olhar mais clínico de quem a tinha de pagar se tornava mais atento. A fraude telefónica na rede fixa tinha o estigma de mundana, pelo que se tornava menos interessante para ser divulgada.

A fraude através de números de valor acrescentado ou audiotexto, onde o custo da chamada telefónica cobrado era mais alto que o normal, foi um flagelo

para os utilizadores, prestadores de serviço e para os operadores de rede que os suportavam. A publicitação de números no jornal local, a oferta de resultados de concursos, de previsões meteorológicas, de conversas privadas com pessoas exuberantes e de roupa reduzida, que ainda existem, mas de outra forma, foram um chamariz para os mais incautos.

O acordo entre o prestador de serviço e o operador de suporte para fornecer um serviço de tarifa superior resultava numa divisão de receita entre ambos. Normalmente, essa partilha de uma parte dos proveitos ocorreria se o operador conseguia ou não receber do chamador. E isso ocorria porque o prestador de serviço de linhas de valor acrescentado ou audiotexto não podia garantir que todos os chamadores fossem verdadeiros e legítimos. Enquanto a maioria deste tipo de prestadores são, no geral, honestos, uma pequena minoria explora esse cenário, gerando chamadas telefónicas massivas, caracterizadas como de fraude, eventualmente para os seus próprios números, aumentando assim o volume geral de chamadas telefónicas estabelecidas e, consequentemente, a receita do operador de suporte que depois repartirá com o prestador de serviço.

Mas, conforme discutido, a fraude como processo sofisticado, por vezes, é tão simples e básica que quase parece uma cena de filme mudo a preto e branco. A fraude por *clip-on* era uma das técnicas mais antigas. Envolvia simplesmente anexar uma ligação telefónica, geralmente com «clipes jacaré», a uma linha telefónica de um operador. E podia ser usada para fazer chamadas telefónicas de saída, ou de entrada, que seriam depois cobradas ao proprietário ou assinante legal do prestador de serviço. Esse tipo de fraude básica era (ainda é?) especialmente comum em países menos desenvolvidos, onde a implantação de rede aérea é abundante e a penetração de linhas telefónicas é baixa.

Existe uma área de fraude muito importante, com literatura publicada e cursos de combate à mesma, cujo elo mais fraco são as pessoas. Este é um assunto tabu, sobre o qual os agentes do mercado de telecomunicações não falam. Infelizmente, a experiência mostra que o envolvimento das pessoas em fraudes ou, pelo menos, a negligência de um ou outro elemento da equipa, pode contribuir para as fraudes bem-sucedidas. Trata-se de um componente importante com uma percentagem substancial em todos os casos de fraude. Pessoas descontentes, corrompidas, em troca de sabe-se lá o quê, pessoas que conhecem pessoas e que, por vezes, não sabem estar... departamentos sensíveis e importantes para a estratégia de negócio de quem está ou pretende realizar determinada fraude, departamentos de crédito, prestação de serviços a terceiros, entre outros, são exemplos de que as pessoas são o elo mais fraco da cadeia de valor. E os funcionários dos fornecedores de equipamentos que, devido às capacidades tecnológicas existentes e salvaguardados por qualquer contrato de manutenção de prestação de apoio imediato, remotamente, acedem ao parque tecnológico a gerir os seus próprios serviços (?). Para os autores da fraude, este tipo de pessoas, com os conhecimentos tecnológicos e o acesso a infraestruturas de outros, poderiam, se assim o quisessem, ser alvos de recrutamento e atividades menos claras ou proporcionar oportunidades de efetuar chamadas telefónicas que não iriam pagar, mas cujos custos alguém iria suportar.

Vivemos num mundo globalizado, numa sociedade que já não é só de informação e onde a tecnologia domina todos os parâmetros da nossa vida social e profissional. A esmagadora maioria da comunicação é efetuada através da Internet, independentemente do tipo de canais utilizados. Vivemos num mundo globalizado

e de redes sociais, onde as organizações estão presentes, sendo a informação, para elas, um ativo crítico.

As vulnerabilidades surgem diariamente pelo que, com o desenvolvimento tecnológico e com o constante aparecimento de novos sistemas, é razoável considerar que novas vulnerabilidades existirão e, portanto, novos tipos de ataques também estarão constantemente a ser criados e desenvolvidos. As redes sem fio, por exemplo, trazem enormes benefícios para os utilizadores, mas também apresentam outras vulnerabilidades que podem colocar em risco a informação crítica. As organizações têm vindo a colocar o enfoque da segurança de informação na segurança física e na segurança lógica. Sistemas e políticas de segurança inovadores são implementados diariamente, cada vez com maior rigidez e menor liberdade para o utilizador. Mas, como atrás referido, é constantemente esquecido o elo mais fraco desta cadeia, aquele que é altamente suscetível a erro e muito permeável, o fator humano. Estamos a falar de engenharia social, que pode ser definida como a arte de «enganar» pessoas, a utilização de um conjunto de técnicas de persuasão, influência e manipulação, com o objetivo de conseguir de forma voluntária informação considerada crítica.

Existindo vários tipos de ataques, obviamente que existem várias formas de os prevenir. Todos os colaboradores de uma organização, sem exceção, são alvos potenciais de engenharia social, ou seja, não existe um grupo específico de indivíduos que se dedicam a este tipo de práticas. Por isso, para além de todas as seguranças tecnológicas, as empresas devem diminuir os riscos do elemento humano através do esclarecimento, educação e treino dos colaboradores. Deve ser dada especial atenção e ter cuidados reforçados com os colaboradores desmotivados, em *outsourcing,* com os que saem voluntariamente e com os alvos de despedimento.

Ataques de engenharia social são eficazes numa vasta variedade de formatos, desde a simples procura de informação no lixo, a métodos verdadeiramente persuasivos, onde a interação do atacante é mais visível, de que são exemplo conversas telefónicas onde é efetuada captura de informação privilegiada. O indivíduo que se dedica a este tipo de atividade vai fazer passar-se por outra pessoa, assumir outra personalidade e fingir que é um profissional de determinada área. Não vai necessitar de forçar ou explorar os erros que possam existir em determinadas máquinas. Ele vai explorar as falhas de segurança das próprias pessoas que, quando não possuem formação para tal, ou não se encontrem formatadas para aquele tipo de evento, podem facilmente ser manipuladas. Este tipo de ataque visa explorar o elo mais fraco da corrente de segurança que é o ser humano.

Existem dois tipos clássicos de ataques de engenharia social: os diretos e os indiretos. Os primeiros são aqueles em que o atacante entra diretamente em contacto com a vítima por correio eletrónico, telefone, ou pessoalmente, tendo um alvo fixo, ou seja, o indivíduo sabe exatamente quem atacar, como e porquê.

Os ataques indiretos não têm um alvo específico, mas aproveitam-se da curiosidade normal do ser humano. É exemplo disso o caso de muitas organizações que enviam informação para o lixo sem a destruir eficazmente, descurando completamente o aspeto confidencial que essa informação possa conter e que pode vir a ser útil a quem a encontrar.

Após a utilização dos métodos anteriores e, face à sua ineficácia, o passo seguinte pode passar pelo acesso direto à pessoa, que é uma metodologia mais difícil de realizar. A sua utilização merece alguma seriedade na composição do

papel e algum planeamento na falsificação de identidade para obtenção da tal informação tão requerida. Aqui, importa saber com quem se está a lidar, pelo que se deve possuir informação mais completa sobre o alvo. Nesta técnica também é utilizada a sedução. Trata-se de uma estratégia de longo prazo que permite um estudo aprofundado do alvo (hábitos, gostos, fraquezas...). A ideia é fazer a aproximação ao alvo e obter a sua amizade explorando a boa vontade para obtenção de favores. Associado a isso, pode ainda ser desenvolvida relação de natureza sexual para obtenção de maior confiança.

De forma direta ou indireta, é fácil concluir que segurança, seja ela digital ou não, é mais do que tecnologia. Os maiores riscos envolvem aspetos humanos, explorados pela engenharia social, que só podem ser minimamente combatidos através da educação. Os colaboradores devem perceber a importância da segurança da informação e ter conhecimento da existência de pessoas preparadas para beneficiar de qualquer fragilidade apresentada pelos sistemas. É importante apresentar os dois lados da história quando abordamos a segurança dita digital. Desta maneira, as pessoas serão menos suscetíveis aos ataques e, estando envolvidas nos processos de segurança, vão compreender e assumir comportamentos mais cautelosos.

A engenharia social é um dos desafios mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação e da fraude em telecomunicações. A sua gestão é um assunto que está em constante mudança, mas que é crítica para as organizações que querem manter a informação confidencial, íntegra e disponível.

Face a uma das ameaças mais antigas do mundo, considerando que a abordagem da serpente a Eva, no Éden, foi a primeira forma de engenharia social, atualmente utilizada para atacar vulnerabilidades dos sistemas informáticos, a melhor maneira de proteger as organizações e os colaboradores das técnicas de engenharia social, bem como o combate à fraude, é a educação e a formação, de modo a estimular a atenção e o bom senso para a não divulgação de informação que possa prejudicar a segurança da organização.

O nosso país não está completamente desperto para os ataques aplicacionais de engenharia social pelo que, em jeito de recomendação para evitar fraudes por engenharia social, deve ser dada atenção à formação, já que as pessoas tornaram-se crédulas e ingénuas relativamente às novas tecnologias (alguns já deram os códigos bancários, outros caíram no conto do vigário dos emails que recebem, entre outras vigarices), aos gastos de dinheiro em tecnologia e menos nas pessoas, aposta em práticas, procedimentos e cultura de segurança, atenção redobrada às atividades de compra de informação, de espionagem industrial, furto de identidade e de dados. Quando alguém entra na organização e diz pertencer a determinada entidade, o português acredita. Ninguém confronta uma pessoa estranha. Nós acreditamos em tudo e todos. É muito fácil fazer-se passar por outra pessoa e furtar ou usurpar uma identidade.

As pequenas empresas estão menos preparadas e são mais vulneráveis. No entanto, todos se conhecem e é mais fácil detetar indivíduos suspeitos. A comunicação é facilitada e pode ser reportada atividade suspeita, pelo que o treino e formação são mais fáceis de realizar devido ao reduzido número de trabalhadores.

As grandes empresas são mais fragmentadas por haver mais indivíduos estranhos a circular no seu interior. Existe também o fenómeno efeito espectador — deixar que outros atuem. Nestas empresas, a comunicação é debilitada porque

normalmente o colaborador não conhece nem interage com os responsáveis da segurança.

É preciso bom senso. A organização deve estar atenta quando recebe uma comunicação do exterior, seja por telefone, correio eletrónico, carta ou até mesmo pessoalmente. Importa ainda que esteja preparada para reagir a eventuais ataques de alguém que pretenda obter determinado tipo de informação.

É importante que se reconheça a natureza convergente da fraude no mercado de telecomunicações. O facto de se poder trabalhar para uma operadora de telefonia móvel não significa que as técnicas de fraude associadas à rede fixa não sejam de nosso interesse. O que fazer caso o nosso telefone de rede móvel esteja a ser utilizado em qualquer parte do mundo, eventualmente a atacar uma central telefónica de uma grande organização? Alternativamente, o que acontece ou o que fará se o mesmo estiver a ser usado em fraude relacionada com numeração de valor acrescentado? O que fazer a seguir? Que preocupações vou ter? E se fosse consigo?

Podem equacionar-se várias técnicas de fraude em telecomunicações que não foram listadas. Na realidade, uma lista abrangente de métodos de fraude poderia preencher um livro, mas o abordado foram tão somente casos simples e escalonados no tempo, nestes últimos 30 anos de desenvolvimento das telecomunicações em Portugal.

Os autores de fraude também são humanos e, por isso, não se consegue prever com segurança quais são suas ações precisas. Mas podemos, se entendermos os seus motivos e ambiente, prever uma possível gama de ações e identificar as ferramentas e técnicas de que necessitamos para responder a cada uma dessas ações. Existem escolhas bastante importantes a serem efetuadas em relação à alocação de recursos limitados para a tarefa e à natureza do pessoal a ser recrutado para tratar do problema da fraude. Para chegar a um conjunto racional de conclusões, é necessário adotar uma visão desapaixonada do autor de fraude como um homem de negócios motivado principalmente pelo lucro, e não como um criminoso perverso que pretende destruir a organização inserida no mercado de telecomunicações.

A experiência evidencia que somente numa minoria muito pequena de casos — ex-funcionários descontentes, sendo os culpados típicos —, as fraudes de telecomunicações são cometidas por malícia.

Importa enfatizar a necessidade de uma abordagem colaborativa para o planeamento estratégico que tenha em conta as preocupações com a fraude. A redução de perdas é um mecanismo legítimo para o aumento de receita, mas não é, em si, uma atividade geradora de receita. Cooperação e coordenação são o nome do jogo. Seja na introdução de métodos preventivos, no fornecimento de estatísticas, no relato de eventos suspeitos ou simplesmente no apoio a investigações internas, praticamente todos os departamentos da organização estarão, em algum momento, envolvidos no combate à fraude. Esta é, portanto, uma iniciativa de toda a organização, que pertence apenas nominalmente à equipa que combate fraudes. Na verdade, um dos principais papéis da equipa de fraude será educar e sensibilizar o resto da organização para o seu papel coletivo na luta contra este flagelo. De facto, a experiência sugere que uma combinação de habilidades é essencial. Polícias, técnicos de telecomunicações, especialistas em *software*, entre outras valências, podem trazer conhecimentos relevantes e úteis para a equipa. Nenhum programa de combate à fraude será considerado

um sucesso, a menos que se possa demonstrar esse sucesso usando meios estatísticos.

Em jeito de conclusão, a consciência das apreciações e das motivações dos autores de fraude são as chaves para o desenvolvimento de uma estratégia bem-sucedida. Pensamento flexível e apoiado superiormente, além da existência de uma equipa motivada, qualificada e comprometida, vêm em seguida. A comunicação interna eficaz é a cereja no topo do bolo. Os sistemas de informação e outros produtos são ferramentas que podem fornecer suporte essencial para a equipa, mas se esses outros princípios forem ignorados, o valor dessas ferramentas será drasticamente reduzido.

O mundo é *cyber*. *Cyberterrorismo*, *cybercrime*, *cibersecurity*, crime digital, *e-crime*, crime eletrónico, integridade, privacidade, disponibilidade, *hackers*, *phreakers*, piratas, são termos associados a uma panóplia de eventos tecnológicos onde se inclui a fraude tecnológica ou de alta tecnologia como agora se gosta de nomear.

Existem outras áreas igualmente apetecíveis para o desenvolvimento de eventos de fraude em telecomunicações, de que são exemplo os videojogos e o acesso a sinais codificados de televisão pelos diferentes métodos. Todos eles são combatidos por indivíduos com algum conhecimento ou troca de informação em circuitos reduzidos.

A emergência da inteligência artificial e das redes de alta velocidade fixa e/ou móvel de alto débito levam o tema da fraude para outro patamar desafiante e estimulante que importa acautelar e combater. É verdade que são temas novos e bastante noticiados, mas também é verdade que há muitos que opinam sem terem a noção do que estão a dizer ou do que vai resultar quando as mesmas estiverem implementadas.

Muito mais haveria a dizer sobre este fascinante e complexo tema da fraude em telecomunicações, mas, nesta abordagem necessariamente sumária, limitei-me a esboçar um breve enquadramento do tema e a chamar a atenção para as debilidades associadas e os possíveis mecanismos de combate.