



# Espionagem econômica:

## o comércio ilegal de informações corporativas

Por Guilherme Martins

**A**s espionagens econômica e corporativa são tão antigas quanto a própria economia. No entanto, a era da internet tornou essa prática ainda mais perigosa para as empresas. A atividade consiste em colher dados sigilosos de empreendimentos de forma ilícita e usá-los contra a instituição ou mesmo vendê-los. Porém, as empresas nem sempre sabem quando são vítimas dessa prática.

Apesar de os dois termos serem usados como equivalentes, há uma diferença entre a espionagem econômica e a corporativa. Na primeira, há uma interferência do país para obter informações financeiras, comerciais, econômicas ou tecnológicas para influenciar decisões políticas de outros países, geralmente com auxílio de serviços de inteligência. No segundo caso, empresas ou corporações utilizam os próprios funcionários para fazer o serviço, ou contratam empresas ou agentes especializados nesse tipo de investigação.

Para diretor da empresa especializada em segurança Velours International, Laurent Serafini, empreendi-

mentos podem ir à falência se tiverem dados roubados. "Pense em uma empresa média com um produto inédito, que gasta anos e dinheiro em pesquisa e desenvolvimento. Um roubo sobre seu trabalho acaba com ela, porque talvez ela não tenha como desenvolver um novo produto. Na França, uma pesquisa revelou que metade das pequenas e médias empresas vítima de um roubo de dados em pesquisa e desenvolvimento quebrou nos dois anos seguintes", afirma.

Serafini explica que a espionagem não está só nos países desenvolvidos. As empresas brasileiras também sofrem ataques, mas subestimam essa prática. "Notamos despreparo e falta de atenção de nossos clientes. As informações hoje podem ser descobertas por simples telefonemas e funcionários desatentos".

O diretor explica que hoje os ataques podem vir de qualquer lugar e, por isso, é necessário reforçar a segurança dos dados. "Hoje pode-se contratar especialistas de alto nível por menos de 400 dólares por dia para roubar informações via internet. Além disso,

há a velha técnica manual de roubo de documentos e materiais. Uma cópia, uma foto com o celular, o uso de um pendrive e o roubo de um carregamento. Há ainda um modo mais simples e sem custos: o *social engineering*, por meio do qual se fazem contatos com uma empresa, com abuso de confiança, manipulação e com identidade falsa, via telefone, correios eletrônicos, correios simples ou fisicamente, para obter informação, dados e destabilizar a empresa.

#### Como proteger sua empresa

O diretor da Velours International, Laurent Serafini, dá algumas dicas sobre como proteger sua empresa:

- O primeiro passo é admitir o risco e ter consciência de que todas as empresas estão suscetíveis a ataques. É fundamental reconhecer essa fragilidade, para evitar que o ataque ocorra;
- Efetuar uma auditoria da empresa nas questões de segurança e dos procedimentos internos. Esse tipo de auditoria, permitirá um mapeamento global dos riscos e vulnerabilidades que será o ponto de partida da atuação. A partir disso, pode-se realizar planos gerais de segurança;
- Por último, deve-se orientar os colaboradores a adotar comportamentos que permitam evitar a perda e a divulgação de informação involuntariamente. Além disso, ficar sempre atento às técnicas dos espões e fraudadores. 🔒

