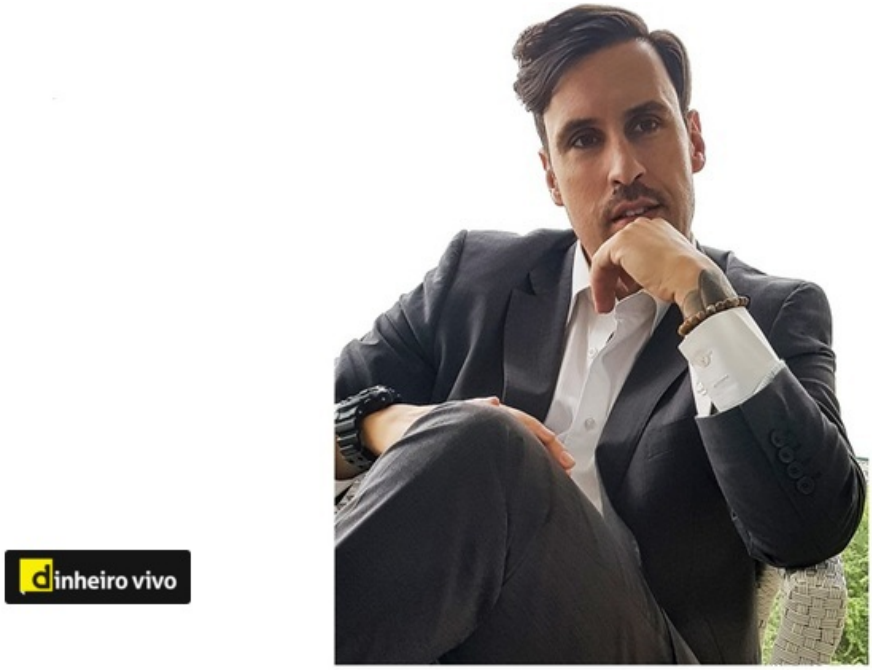
# Engenharia Social: como o (ciber)crime se tem reinventado

dinheirovivo.pt/opiniao/engenharia-social-como-o-cibercrime-se-tem-reinventado-12773375.html

27 de setembro de 2019




Todos sabemos que o cibercrime é uma realidade que veio para ficar e que tem crescido exponencialmente, um pouco por todo o mundo. Portugal, naturalmente, não é exceção.

E ainda que não seja possível considerar que as empresas portuguesas já têm um grau efetivo de maturidade no que diz respeito à (ciber)segurança, já não se pode dizer que estão completamente alheias aos riscos do ciberespaço.

É precisamente a consciência de que as empresas já despertaram para o cibercrime que tem levado "criminosos" por todo o mundo a reinventarem-se e a sofisticarem os seus métodos de ataque para que as empresas continuem a perder milhões, mesmo depois de investirem em tecnologias de defesa, ou implementarem políticas de segurança de informação e até corrigirem vulnerabilidades de segurança.

Costumo dizer que o elo mais fraco das organizações é o indivíduo e, por isso, incentivo os meus clientes a apostarem fortemente em formação. Uma formação que deve ser feita de forma regular e direcionada a todos os colaboradores de uma organização, sem exceção, já que as ameaças são cada vez mais sofisticadas e cada vez mais orientadas para o elo mais fraco, sendo essa vulnerabilidade o "erro humano".

Temos verificado com alguma surpresa um regresso aos métodos "*old school*" de engenharia social, pura e dura, para perpetrar ciberataques potenciados por tecnologia de ponta. A engenharia social, termo que pode ainda ser desconhecido ao leitor, mais não significa do que manipulação. Figuras que ficaram "famosas" por perpetrar enormes ataques nos anos 90, como Kevin Mitnick, orgulhavam-se de contornar grandes barreiras

de segurança de empresas gigantes com o exclusivo uso da palavra. Bastava, para isso, estudar o alvo que serviria de porta de entrada, e, posteriormente, utilizar esse conhecimento aliado a técnicas de manipulação “verbal”.

Nessa altura, vasculhava-se o lixo, colocavam-se escutas, faziam-se chamadas em que os criminosos se faziam passar por outra pessoa… tudo com o objetivo de criar um perfil para, posteriormente, iniciar um contacto que se presumiria de confiança e seguro.

Hoje, acresce que o enorme desenvolvimento da “tecnologia” permite levar a engenharia social para outro patamar de escala e sucesso.

Tome-se por exemplo uma empresa que tenha sofrido um ciberataque e que vê todas as suas bases de dados encriptadas até ao pagamento de um resgate (*ransomware*). Vamos supor que a empresa decide pagar o resgate e que os criminosos “até foram gentis” e disponibilizaram, de novo, o acesso à informação. A empresa decide, para evitar situações futuras, investir finalmente em cibersegurança. Ora, um ano depois, poder-se-ia considerar que era uma empresa minimamente segura e que o incidente já faria parte de um passado longínquo.

Acontece que aquela informação, outrora encriptada, não deixou de ser comprometida.

Imagine-se que o criminoso decide estudar toda a informação outrora roubada e consegue, a partir daí, descodificar as relações internas da empresa, a forma como se comunica, que circunstâncias geram transferências, quem é quem e que papel desempenha na organização, como fala, que fraquezas tem. Basta uma chamada para a pessoa certa, um *email* aqui e ali que faz lembrar os antigos esquemas de burla e… *voilá*, a empresa acaba outra vez por ser “ludibriada” e por ser vítima de roubo de milhões sem ter sequer entendido como nem por quem.

Este pode ser um exemplo com contornos "simplistas", mas é bem real e cada vez mais popular.

Este fenómeno deve servir para alertar não só as empresas que não investem em cibersegurança como aquelas que, investindo, têm a ilusão de que a cibersegurança é garantida com uma ação pontual. A segurança é, e será sempre um processo de avaliação e melhoria continua.

Afinal, apesar de este tipo de ataques implicar um enorme esforço de análise, que demora bastante mais tempo do que o necessário para os perpetrar se a recompensa valer o esforço, o criminoso seguirá em frente.

*Bruno Castro é CEO da VisionWare*