manchete

Diário Notícias
Insider
22-07-2018

Periodicidade: Diario
Classe: Informacão Geral
Âmbito: Nacional
Tiragem: 56361
Temática: Banca/Seguros
Dimensão: 694 cm²
Imagem: S/Cor
Página (s): 54


Cibercrime já é mais rentável do que o crime organizado

OPINIÃO

Cibercrime já é mais rentável do que o crime organizado

SOFIA TENREIRO

Diretora-geral da Cisco Portugal

Willie Sutton foi um famoso assaltante de bancos do século passado que, quando interpelado sobre o motivo para continuar a escolher os bancos para assaltos respondia: "Porque é nos bancos que o dinheiro está guardado." Hoje, o dinheiro está *online*. Não só os bens materiais têm presença *online* como há muita informação *online* que tem valor incalculável, por si só ou pela importância para quem a detém.

O cibercrime é, por isso, já mais rentável do que o próprio crime organizado, estimando-se que represente entre 450B e 1T de dólares por ano. E é um negócio em crescimento, havendo cada vez mais ataques e mais sofisticados, que exploram as fragilidades dos sistemas e do próprio homem. Quer a nível profissional quer a nível pessoal, devemos ter o máximo de informação para sabermos como nos proteger. Por exemplo, hoje os *hackers* estão a deixar de "roubar" informação para a alterar prejudicando assim a sua integridade. Hoje também estão a usar, cada vez mais, inteligência artificial para melhor conhecerem os seus *targets*.

Para combater esta realidade, há cada vez mais investimento a ser canalizado, por parte das grandes tecnológicas, em talento (Hackers for Good) e em desenvolvimento de soluções tecnológicas. Estes são os "polícias" que zelam por nós e pelas nossas empresas. Mas hoje, tão importante como estar protegido contra os atacantes, é ter mecanismos que nos permitam perceber que fomos atacados o mais rapidamente possível para bloquearmos o ataque e repormos a situação. Parece óbvio mas, infelizmente, cem dias é ainda a média do mercado para esta deteção. Em cem dias, o que não pode um *hacker* descobrir e roubar? Felizmente que, através da visibilidade da infraestrutura das nossas empresas, já é hoje possível reduzir esse tempo para pouco mais de duas horas. Mas, para isso, as empresas têm de apostar em soluções que lhes permitam ter uma infraestrutura inteligente e segura.

A nível pessoal é também importante garantir que se investe neste tipo de soluções. Porém, o fator humano é ainda uma das maiores fragilidades que abrem as portas ao *malware*. Por isso, é importante ficar atendo às formas de ataque mais conhecidas (*e-mails* e anexos desconhecidos, pedidos de informação fora do normal, visita a *sites* infetados, etc.). Os *hackers* são pessoas e, como tal, exploram os comportamentos humanos procurando criar estratégias que não sejam detetadas (por exemplo, um *e-mail* recebido de um colega de trabalho ou de um amigo pode não ser verdadeiro e conter um anexo com *malware*). A sua criatividade não tem limites.

Estima-se que no ano 2020 já cerca de 50 mil milhões de equipamentos estejam conectados, o que, por um lado, maximiza o potencial de negócio e o impacto positivo que poderemos ter nas nossas vidas, mas, por outro, aumenta exponencialmente os riscos de ataques cibernéticos. Teremos cada vez mais eletrodomésticos e equipamentos de lazer ligados *online*, pelo que temos de garantir que também estão protegidos.

Em conclusão, devemos adotar uma postura em relação à cibersegurança semelhante à da segurança física. Se nunca saímos de casa sem trancar as portas, devemos ter os mesmos cuidados com a internet, apostando na prevenção. Temos não só de investir em tecnologias que nos permitam estar protegidos mas também ter uma atitude atenta às ameaças existentes.

Os *hackers* são pessoas e, como tal, exploram os comportamentos humanos para criar estratégias que não sejam detetadas.