“Ciberataques silenciosos são mais perigosos”

Edward Stroz, vice-presidente da consultora AON e ex-agente do FBI, diz que **um dos próximos alvos dos *hackers* vai ser a integridade dos dados**

O Petya atacou na passada terça-feira várias empresas europeias e americanas. Os países mais atingidos foram a Ucrânia e a Itália
FOTO GETTY IMAGES

Os últimos ataques de *ransomware* — o Wannacry, ocorrido no final de maio, e o Petya, noticiado esta terça-feira — não são os mais perigosos, defende Edward Stroz, vice-presidente da AON, empresa britânica especialista em gestão de risco. “Os ataques silenciosos, que de forma discreta roubam informação, são bem mais perigosos”, afirma este norte-americano, que foi durante alguns anos agente do FBI na área da criminalidade financeira. Já os ataques de *ransomware*, acrescenta, são pensados para serem mediáticos e espetaculares, porque se difundem depressa e foram desenhados para encriptar dados e pedir um resgate. “Podem ser facilmente prevenidos se tomarmos as medidas adequadas, como ter versões de software atualizadas que evitem as vulnerabilidades e cópias de proteção *offline*.”

Apesar de haver cada vez mais ameaças, Stroz diz ser possível que as empresas tenham um grau elevado de imunidade aos ciberataques se adotarem o que apelida de higiene digital. “Funciona como a higiene pessoal: para não sermos atacados por bactérias, devemos lavar as mãos. No mundo digital, também é importante ter as versões atualizadas de software, nomeadamente os *patches* de segurança. E é essencial fazer cópias de segurança de forma regular, para poder repor os dados em caso de ataque.”

Questionado sobre a segurança da nuvem, este especialista diz que, em princípio, a colocação dos dados num bom prestador de serviços na nuvem é mais seguro do que tê-los apenas no computador. “Em caso de ataque a um computador, será mais fácil recuperar os dados se eles estiverem na nuvem”, sublinha.

Ataque aos dados

Depois de sair do FBI, Ed Stroz fundou a consultora Stroz Friedberg, que, no final de 2016, foi vendida à AON. Observador atento do cibercrime, Stroz tem conseguido antecipar algumas vagas de crimes cibernéticos, como os ataques à confidencialidade dos dados (por exemplo, cópias de números de cartões de crédito) e o fenómeno *ransomware* (Wannacry e Petya). Onde é que os *hackers* vão atacar a seguir? “A qualidade e a integridade dos dados vão ser os próximos alvos”, antecipa. Ou seja, os criminosos vão querer alterar a informação. Tal como as notícias falsas procuram informações não verdadeiras, corromper os dados dá origem a manipulações ainda maiores. Há que ter estratégias para minimizar os riscos, alerta.

A qualidade e a integridade dos dados vão ser os próximos alvos dos *hackers*

Há um grande potencial de perigo de ataques aos carros autónomos. É um novo território, que vai colocar novos desafios às companhias de seguros

Os *hackers* vão poder usar a internet das coisas como plataforma de lançamento para atacar outras redes

EDWARD STROZ
Vice-presidente da AON

Uma das medidas que ajuda a gerir estes perigos nas grandes empresas é a criação de um departamento de segurança, coordenado por um diretor de segurança, ou CSO (Chief Security Officer). “É preciso criar um modelo de governação patrocinado pela gestão de topo que possa identificar as ameaças e estabelecer as prioridades. É preferível que não fique sob a alçada do departamento de informática”, defende o vice-presidente da AON. E recomenda que este departamento faça com que todos os empregados tenham preocupações com a segurança. “Se alguém faz uma cópia de um ficheiro para uma conta individual de Gmail, essa não é uma questão que o departamento de informática consiga controlar”, exemplifica.

Com que objetivos atua o cibercrime? Ed Stroz diz que muitos *hackers* procuram ganhar dinheiro e outros atuam por motivações políticas e pessoais. E alerta: “Um computador pode ser programado de acordo com a lógica que se pretender. É cada vez mais fácil ter acesso a *malware* no grande mercado da chamada *dark web*.” Estão disponíveis no lado obscuro da internet componentes que podem ser usados mesmo por quem não for um técnico e até criar *interfaces* muito amigáveis com o utilizador. “Quando a oferta e a procura se encontram, o poder do mercado aumenta, aumentando também os danos que podem ser feitos”, adverte.

Perante esta facilidade de acesso a software malicioso, Stroz diz que os governos têm de saber balancear a privacidade dos cidadãos e a segurança. “É uma questão complicada, porque cada parte tem legitimidade nos argumentos. Cada país tem os seus serviços secretos, que procuram encontrar formas de proteger a sociedade e desempenhar a sua missão. Não consigo dizer que lado tem razão: é preciso fazer um balanço, não num laboratório mas sim num debate na opinião pública. Os Estados devem criar uma legislação equilibrada que não ponha em causa a privacidade dos cidadãos. Ter uma câmara para vigiar uma criança é legítimo, mas se forem usadas para vigiar a casa já pode ser problemático.”

Novas frentes

A internet das coisas e os carros autónomos são duas tecnologias emergentes que podem fazer aumentar os ataques, admite Stroz. “Há uma enorme quantidade de código que suporta a tecnologia dos carros autónomos. Há um potencial perigo de alguém corromper o código e sequestrar o carro.” Esta nova tecnologia irá colocar desafios às companhias de seguros. “É um novo território. Vai mudar a forma como encaramos hoje um acidente de automóvel. Já não é o ser humano a controlar o carro, mas sim código de software.”

Já na internet das coisas, a questão é diferente. “O principal perigo é que essa rede de sensores pode ser usada para atacar outras redes. “Um ar condicionado de um edifício inteligente pode ser uma plataforma de lançamento e afetar centenas de equipamentos de uma empresa”, garante Stroz.

JOÃO RAMOS
jramos@expresso.impresa.pt

Ataque Petya

Esta semana, algumas empresas europeias foram vítimas de mais um ataque de *ransomware*. Este software malicioso, conhecido por Petya, espalhou-se através de grande empresas, como a agência de publicidade WPP ou a companhia de transportes marítimos dinamarquesa Maersk. O país mais atingido, segundo a empresa de segurança ESET, foi de longe a Ucrânia (onde afetou um banco, um aeroporto e uma energética estatal), seguido pela Itália, Israel e Sérvia. O impacto em Portugal foi diminuto. Depois do Wannacry, este é o segundo ataque global do género em menos de dois meses. Os cibercriminosos encriptam ficheiros e pedem um montante em *bitcoins* de perto de €300 como resgate para que os utilizadores tenham a informação de volta. Ed Stroz desvaloriza o perigo do *ransomware* e recomenda às empresas vítimas que não paguem os resgates. O Petya distingue-se por se ter propagado nas redes das empresas, não percorrendo a internet através de componentes externos como o correio eletrónico, tal como tinha acontecido com o Wannacry.

DESAFIOS DO DIGITAL

Software atualizado
Para evitar um ataque é fundamental instalar nos equipamentos versões atualizadas de software, nomeadamente os chamados *patches* de segurança.

Cópias de segurança
É essencial fazer cópias de segurança regularmente em equipamentos não ligados à internet, de forma a melhorar a capacidade de recuperação de dados em caso de ataque.

Nuvem
Usar um serviço de computação na nuvem é, em princípio, mais seguro do que ter os dados nos computadores existentes nas instalações da empresa.

Eleições
“Hoje, é possível manipular um processo democrático de diferentes formas, desde divulgar informação falsa a atacar os mecanismos de recolha de dados eleitorais ou os registos de eleitores. Não há nenhuma democracia que esteja a salvo destes ataques”, diz o vice-presidente da AON.

Diretiva de privacidade
A diretiva europeia de proteção de dados — General Data Protection Regulation (GDPR) — é, para Ed Stroz, “uma medida legítima de zelar para que as pessoas tenham privacidade no mundo digital, porque a tecnologia traz novos riscos”.