Expresso
18.02.2022

Duelo Especialistas dividem-se se PJ e SIS conseguem suster as redes de *hackers* que têm atacado em força os sistemas informáticos de grandes empresas em Portugal

Jorge Bacelar Gouveia

Presidente do Observatório de Segurança, Criminalidade Organizada e Terrorismo; e constitucionalista

Bruno Castro

Fundador e CEO da VisionWare, especialista em cibersegurança e investigação forense

AS AUTORIDADES ESTÃO PREPARADAS PARA ESTA ONDA DE ATAQUES INFORMÁTICOS?

SIM

O ciberespaço há muito que deixou de ser um tema de ficção científica e tornou-se uma realidade, ainda que incorpórea, que a todos diz respeito e condiciona.

Mas enfrenta-se agora uma nova fase, em que se perdeu a "inocência" no ciberespaço, se inicialmente entendido para fins lúdicos, didáticos ou de comunicações.

É cada vez mais evidente o seu "lado obscuro", no qual se multiplicam as atividades ilegais — muitas até criminosas — que põem em causa os direitos das pessoas e a estabilidade das instituições, nacionais e internacionais.

Eis que a 4ª Revolução Industrial — depois da invenção da máquina a vapor, da produção em série e da utilização dos computadores — aí está, com os seus benefícios ligados à inteligência artificial (IA), a qual pode ser chamada a desempenhar um papel relevantíssimo em matéria de segurança informática.

Porém, não é só a IA que terá essa tarefa: as autoridades públicas igualmente têm levado a cabo um esforço nessa direção.

Desde logo, cabe mencionar o pioneiro regime jurídico da segurança do ciberespaço, impondo a serviços públicos e entidades privadas planos de proteção contra ciberataques, podendo as mesmas ser penalizadas com coimas no caso de aquelas regras não serem cumpridas.

Enfrenta-se agora uma nova fase, em que se perdeu a "inocência" no ciberespaço

Estes grupos de cibercriminosos são globalizados. O seu 'rasto' disperso dificulta o trabalho das autoridades

É preciso também sublinhar que há todo um esforço discreto que tem sido incrementado a partir de organismos da União Europeia, cuja cooperação se tem intensificado através da adoção de decisões comuns, sendo viável que a luta contra o terrorismo — decerto mais grave do que os ciberataques — possa ajudar a repressão destes, numa relação de simbiose que não é despiciendo e que está a fazer o seu percurso.

E não é só no plano europeu, porque a cibersegurança é um objetivo mundial. O recente e infausto episódio do atentado falhado na Faculdade de Ciências da Universidade de Lisboa veio comprovar, para quem ainda tivesse dúvidas, de que tal cooperação funciona: primeiro, pelo alerta dado pelo FBI; depois, pelo trabalho efetuado pela Polícia Judiciária, que com muita proficiência cumpriu com o que lhe competia.

Ao nível interno, as forças e os serviços de segurança, nos seus campos específicos de atuação, têm trabalhado no acompanhamento das atividades da *deep web* e mesmo *dark web*, com infiltração de agentes e outros mecanismos de intervenção.

Significa isto que tudo está bem? Não. Há muito a aperfeiçoar e a corrigir, sobretudo no reforço dos meios humanos, materiais e tecnológicos, uma vez que a consciência da gravidade dos ciberataques já é uma conquista dos cidadãos e das empresas.

Nunca estaremos totalmente seguros e a segurança em estado puro não existe, pelo que a regra de ouro é nunca baixar a guarda.

É bem certeiro o velho provérbio português: "O seguro morreu de velho e a prudência foi ao funeral."

NÃO

Nos últimos meses temos assistido semanalmente — se não diariamente — a uma intensificação e sofisticação de ciberataques em todos os sectores da sociedade portuguesa. Estes ataques que têm vindo a acontecer têm trazido muita turbulência, visto que, em certos casos, também têm implicado um impacto no *core business* das 'vítimas', e, por inerência, ao próprio sector onde atuam.

O crime cibernético tem sido uma das tipologias que mais tem aumentado desde o início da pandemia, tanto ao nível do volume de ataques registados como de denúncias, reforçando que estas situações continuam sem conseguirem ser travadas pelas entidades competentes, e nelas estão incluídas não só as autoridades que investigam este tipo de ataques como as próprias empresas, que continuam a não dar o devido valor ou investimento a esta área de atuação.

Com o incremento quase explosivo do número de ciberataques, as autoridades não dispõem de recursos necessários para responder a todas as solicitações. Para além de mais ataques, e com sucesso, são também cada vez mais sofisticados, e, portanto, obrigam a um esforço muito superior no processo de investigação por parte das autoridades. Seguir o rasto da pegada digital deste tipo de grupos criminosos, que atuam de forma encoberta, prolongada no tempo e tecnicamente aprimorada, é cada vez mais exigente — tecnologicamente, na capacidade de resposta e conhecimento especializado envolvido — para quem tenta investigar e prevenir este tipo de ciberataques.

Não devemos esquecer que estes grupos de cibercriminosos são globalizados, isto é, sem nacionalidades atribuídas ou espaços físicos associados. O facto de existir um 'rasto' disperso dificulta, e muito, o trabalho das autoridades. A própria legislação, em si, apresenta algumas lacunas, já que abrange contornos complexos quando falamos em cibercrime num contexto onde o planeta Terra é o seu *playground*.

Atualmente, e após o ciberataque (muito prolongado na sua resolução) à Vodafone, percebemos a gravidade da situação, mas principalmente o quão vulneráveis somos às ameaças desta nova era digital em que passámos a viver. Este ciberataque causou uma violenta interrupção de um pilar da nossa sociedade, as comunicações (dados e voz) entre todos nós. Na sequência dos restantes ciberataques ocorridos nos últimos meses, e face ao impacto causado, acrescido de não ter existido qualquer conclusão efetiva da origem, causador e motivação dos mesmos, ficamos com a sensação de que as autoridades estão com dificuldades em concluir com sucesso os vários processos de investigação.

Do nosso lado — VisionWare —, temos vindo a registar um número avultado de solicitações de empresas e instituições, as quais começam agora a preocupar-se com a questão da segurança da informação e da cibersegurança como topo das suas prioridades de gestão. Finalmente, o *chip* está a mudar para todos, pelo que as autoridades competentes terão, de facto, um gigantesco desafio pela frente.