Cibersegurança: O que nos espera em 2020?

dinheirovivo.pt/opiniao/ciberseguranca-o-que-nos-espera-em-2020-12686915.html

28 de fevereiro de 2020

No último artigo de 2019, fiz uma análise retrospetiva sobre segurança cibernética. Chegou agora a altura de refletir sobre o que nos reserva 2020 nesta área.

Parece-me seguro dizer que a ciberameaça não só persistirá como se tornará cada vez mais sofisticada.

Ou seja, continuaremos a assistir aos mesmos ataques, como é o caso do *phishing*, mas em maior quantidade e com mais sofisticação. Ataques cada vez mais orientados à vítima, juntando estratégias de engenharia social e tecnologia de ponta, que poderão ainda fazer-se valer de informação recolhida em ataques anteriores, por exemplo de *ransomware*, para perpetrar ataques muito bem estudados, sustentados e dificilmente detetáveis. Uma tendência que denunciámos em 2019.

Numa outra vertente, mas ainda dentro da persistência da ciberameaça, há que mencionar as já expectáveis campanhas de desinformação e ciberataque direcionadas aos candidatos das eleições norte-americanas, ou a outros eventos de dimensão e relevância global, como está a acontecer a propósito do COVID-19.

Depois, poderão continuar a crescer os mecanismos de resposta por parte das instituições nacionais e internacionais, nomeadamente europeias, que parecem começar a reconhecer o ciberespaço como um território de atuação que comporta tantos ou mais riscos quanto os espaços tradicionais.

O caminho destas entidades deve ser complementado pela iniciativa das próprias empresas que agem no ciberespaço, que não devem aguardar por determinado tipo de políticas ou regulamentos para reforçar a sua segurança. Refiro-me em particular às

entidades que prestem serviços essenciais, as denominadas infraestruturas críticas. A este propósito vale a pena referir que, ainda no passado dia 19 de fevereiro, o Departamento de Segurança Interna dos Estados Unidos revelou que uma instalação de gás natural tinha sido forçada a encerrar as operações durante dois dias, depois de ter sido atacada por *ransomware*, antecedido por um primeiro ataque de *spear-phishing*, via e-mail. Este exemplo é apenas mais um de um ataque cada vez mais frequente e que nos recorda que a cibersegurança deve, antes de qualquer coisa, ser preventiva.

Diretamente relacionadas com as ciberameaças - já que dão o material essencial (dados) para a promoção de determinado tipo de campanhas maliciosas - estão as violações de dados.

Acredito que continuaremos a assistir a fugas massivas, como foi o caso do *leak* único, ocorrido no ano passado, que expôs praticamente toda a população chilena. Estes fenómenos ocorrem por diversas razões, seja por má configuração na utilização de infraestruturas *cloud*, seja por falhas de segurança em empresas terceiras que têm acesso aos dados - de forma legítima ou não - ou pelo aumento da superfície de ataque que as empresas, por vezes, desconhecem, não documentam ou inventariam de forma incorreta. Este último ponto é particularmente importante, já que me refiro não apenas à utilização de SaaS (Software as a Service) e PaaS (Platform as a Service) - como é o caso do Office 365 ou da Microsoft Azure, presente na maioria das empresas - que mais não são do que serviços de *renting* como a Uber, em que, em vez de usarmos um transporte próprio, usamos o de alguém. Refiro-me em particular à utilização abusiva de equipamentos de IoT (*Internet of Things* ou Internet das Coisas).

As pessoas devem perguntar-se porque querem "ligar a torradeira à internet", se de nada serve vivermos numa *smart city*, numa *smart house* ou trabalharmos numa *smart company*, se depois não tivermos uma atitude *smart* face à segurança.

Estamos a chegar a um ponto em que já é muito difícil falar de indivíduos ou organizações realmente anónimas. Mas a atitude perante a inevitabilidade da interconectividade não pode ser a indiferença. E responder com soluções que nos levam de volta ao analógico ou ao *offline* é mais uma desistência do que uma desejada ultrapassagem ao desafio da internet.

Quero acreditar que 2020 será um ano de viragem para a cibersegurança. Estou certo que será um ano de descoberta de novas formas de combate da cibercriminalidade, através de soluções como a sofisticação, a rapidez, a formação e a tecnologia. Em prol da proteção da sociedade civil e das organizações públicas e privadas.

Bruno Castro é CEO da VisionWare