

Aumento de ciberataques com sucesso em Portugal gera preocupação

noticiasao minuto.com/tech/1964886/aumento-de-ciberataques-com-sucesso-em-portugal-gera-preocupacao

March 30, 2022

O especialista em cibersegurança português Bruno Castro assumiu hoje a preocupação com o aumento dos ataques cibernéticos com sucesso a empresas em Portugal desde o início da pandemia, alertando para um pico de casos nos últimos meses.



© iStock



14:43 - 30/03/22 por Lusa

Tech Ciberataque

"Houve imensos casos de ataques cibernéticos desde 2019 com sucesso. Ao contrário do passado, houve muito mais casos de ataques, é verdade, mas ainda muito mais casos de ataques com sucesso. Isto tem muito a ver com a exposição que de repente houve, quer de os colaboradores estarem na Internet, de repente, sozinhos, desprotegidos, e as empresas terem de dar este salto, não preparado", disse, em declarações à Lusa, na cidade da Praia, Bruno Castro, diretor-executivo da VisionWare.

"Nos últimos 20, 25 anos de carreira nunca vi nada assim", reconheceu.

O especialista em cibersegurança português afirma que a situação tem vindo a agravar-se desde setembro, com a multiplicação de casos de ciberataques com sucesso, e mediáticos, a empresas em Portugal, desde logo o realizado à operadora de telecomunicações Vodafone.

"Foi aí efetivamente o ponto em que tudo isto começou, neste novo cenário de ciberterror, em que houve muitos ataques passivos a grandes empresas, em que o nível de maturidade delas é elevado até, e teve um impacto muito violento em termos de disrupção de serviço, e tornou-se mediático", apontou o administrador da VisionWare, uma das mais antigas empresas de cibersegurança em Portugal e líder de mercado, trabalhando internamente com mais de uma centena de empresas em todo o mundo.

A MC, detida pela Sonae, confirmou hoje que "se verificou um ataque informático nos sistemas que está a afetar comunicações nos 'sites' e alguns serviços do Continente.

"Lamentamos os constrangimentos causados", acrescentou a empresa da Sonae na mesma nota, referindo que as suas "equipas estão a trabalhar no sentido de averiguar a perturbação e repor, com a máxima brevidade, o normal funcionamento da atividade".

"Ainda é muito fresco, muito recente, para se falar sobre isso, em horas iremos saber em concreto o que aconteceu. Aparentemente deverá ter havido aqui um ataque vertical feito à parte que é exposta para a Internet, penso que do grupo Continente, na área do Continente, inclusive colocou em causa os pagamentos com cartão do Continente. Poderá ser algo um bocadinho mais profundo que propriamente um ataque meramente à componente que está exposta, 'web', pela Internet", comentou Bruno Castro, questionado pela Lusa sobre este caso, durante a visita de trabalho que está a realizar a Cabo Verde.

Acrescentou que o número de ciberataques às empresas em Portugal é hoje "muito maior", numa tendência cada vez mais vincada desde 2018, agravada pela pandemia de covid-19, que obrigou as empresas, para manterem a atividade, a "dar um salto instantâneo para Internet", ao nível dos colaboradores e dos sistemas internos, mas também do negócio ou das relações com fornecedores e parceiros.

"Isso veio também trazer imensos problemas, porque ligamos milhares de redes domésticas à rede corporativa, dois focos perigosíssimos. Mas era algo que tinha de acontecer, eram formas de sobrevivência dos Estados e das empresas. E, portanto, nesta fase da pandemia senti claramente que os decisores perceberam que tinham de tomar

uma decisão que era arriscada, que era tudo para a Internet (...). Sabiam que era arriscado, mas tinha de acontecer e depois tinham que correr atrás do tempo, logo a seguir", reconheceu.

O especialista destacou ainda o exemplo do ataque, este ano, à Vodafone, uma das "mais evoluídas" empresas em Portugal ao nível da cibersegurança, e que, no entanto, sofreu "um impacto violentíssimo, com um enorme sucesso, que colocou em causa toda a imagem e operação".

"Isto só nos vem alertar para uma coisa: O processo de segurança é contínuo, não é uma coisa estanque, não é uma coisa instantânea, é uma longa caminhada, que nunca acaba", insistiu.

Para Bruno Castro, estes ciberataques lembram a vulnerabilidade global da nova realidade de comunicações: "Temos de saber viver com isso. É uma realidade nova e que no meu entender nunca mais se irá alterar. Nós temos é que gerir este processo de evolução contínua, de gestão do risco, de deteção do risco, minimizar o risco, procurar sempre a última falha. É uma luta muito cansativa, mas que vai ser interminável".

Recordou que há quase 30 anos, quando entrou nesta área, a cibersegurança "era uma coisa estratosférica", mas que passou a ser um tema "muito mais mediático" e "sexy".

"Do lado da Europa tem havido cada vez mais regulamentação que obriga as empresas a implementar a segurança, nomeadamente empresas que tenham serviços críticos para o país, que impliquem a estabilidade, comunicações, banca, água, energias. Isso tudo cada vez mais está a ser regulamentado", reconheceu.

Além disso, sublinhou, há uma "proatividade" dos gestores das empresas com a cibersegurança, porque "estão preocupados" com esta nova realidade.

"Há recomendações que devem ser feitas: literacia dos colaboradores, as empresas serem capazes de, quando estão na Internet, se protegerem devidamente, testarem os seus sistemas vezes sem conta, retestem, voltem a testar e auto avaliem-se continuamente, sem parar. Não deem como bom um processo de auditoria que é feito há cinco anos e fica estanque, esqueçam isso", apontou.

"Tem que ser contínuo, sem parar, e cada vez mais vai ser fundamental montar sistemas inteligentes que também vigiem os castelos das empresas 24 horas por sete dias da semana, à noite quando todos estão a dormir tem de haver alguém de guarda. Esse conceito tem de ser implementado agora, de forma perfeitamente natural, sem ser um luxo", concluiu o diretor-executivo da VisionWare.

