Cibercrime dispara em Portugal. "Já foi roubado muito dinheiro, tem sido assustador"

tsf.pt/portugal/sociedade/cibercrime-dispara-em-portugal-ja-foi-roubado-muito-dinheiro-tem-sido-assustador-12111041.html

24 de abril de 2020

O cibercrime está aumentar em Portugal desde o início da pandemia do novo coronavírus. Só este mês, dezenas de organismos e empresas foram atacados por piratas informáticos.

Já foram alvo de hackers o Ministério da Saúde, o Serviço Nacional de Saúde, o Portal das Finanças, o Ministério da Administração Interna, o Sporting, o Benfica, o Portimonense, a Universidade dos Açores e de Lisboa, a Caixa Agrícola, o BBVA Portugal a EDP e a Altice, entre muitos outros.

Um grupo de piratas informáticos tem em marcha aquilo a que chama "operação 25 de abril" e já anunciou que se apoderou de 86 bancos de dados desde o início de abril.

"Já foi possível roubar muito dinheiro. Tem sido assustador", diz à TSF Bruno Castro.

O fundador da Visionware, empresa especializada em segurança informática, cibercrime e ciberterrorismo que trabalha com vários organismos em Portugal, com a Comissão Europeia e a NATO, conta que em 15 anos no mercado nunca teve tanto trabalho como nos últimos dois meses.

"Diria que estamos a ter um incremento três vezes maior de ataques com sucesso. Nunca tivemos tanto trabalho como agora." O volume de ataques preocupa o especialista em segurança informática, mas principalmente o aumento eficácia. "A taxa de sucesso tem crescido exponencialmente", diz.

"É incrível como ataques bastante conhecidos, como o *phishing*, agora têm tido sucesso ainda maior do que já tinham antes, com pedidos de resgate e ações de fraude monetárias enorme", alerta.

O coordenador da equipa de resposta a incidentes do Centro Nacional de Cibersegurança, Rogério Raposo, diz mesmo que os casos de ataques informáticos a partir de mensagen de correio eletrónico ou de mensagens para telemóveis, aumentaram 300% por cento destde o início do ano.

Riscos do teletrabalho

Bruno Castro dá o exemplo de pequenas e médias empresas, as mais vulneráveis, onde já houve ataques "com cinco ou seis transferências de meio milhão de euros" ao longo de semanas, que não foram detetados até o banco avisar que já não havia saldo na conta.

Os ataques aumentaram devido às fragilidades de segurança inerentes ao teletrabalho, considera Bruno Castro. "Tudo é por email e se eu tiver acesso ao e-mail de uma ou duas pessoas importantes da empresa posso usurpar a sua identidade para ações maliciosas."

A urgência com que foi necessário criar ferramentas para teletrabalho pode ter contribuído "para várias lacunas na segurança", com cenários que as empresas não estavam preparadas para antecipar "porque nem sequer era plausível", nota o especialista. E os "grupos de hackers ou ativistas aproveitaram."

Como proteger empresas e trabalhadores?

Entre os conselhos para evitar ataques e proteger empresas, o especialista sugere que se faça uma avaliação de todos os serviços que estão expostos na internet. Sim, a prioridade foi "colocar a o serviço no ar" para continuar a trabalhar online, mas é preciso, o quanto antes "validar a sua segurança", lembra.

Uma vez corrigidas as falhas de segurança, a segunda fase é proteger os trabalhadores. "Muitas destas empresas estão a ligar centenas de redes domésticas dos seus colaboradores à rede cooperativa", expondo-se a mais ameaças.

Por fim, os trabalhadores devem receber formação para saber o que não podem fazer, mesmo nos momentos de lazer, uma vez que, ainda que fora da hora de trabalho, muitos continuam ligados remotamente à empresa.

Porque demora tanto recuperar um site?

Muitos dos sites de organismos públicos que foram atacados continuam em baixo ao fim de vários dias. Bruno Castro explica o porquê da demora: é preciso abrir um processo de investigação forense para apurar responsabilidades e perceber como é que os piratas informáticos se infiltraram, "até onde foram" e "onde é que andaram, o que é que acederam, o que é que roubaram, o que é que alteraram".

"Esta análise tem de ser feita imediatamente e durante a investigação a regra é desligar os serviços todos", explica. Depois é preciso corrigir todas as falhas de segurança e repor os serviços com "um reforço de segurança".

Crianças "passeiam" num mundo perigoso

Bruno Castro mostra-se ainda muito preocupado com as crianças que agora passam mais tempo em casa e que, ao contrário do que se possa pensar, estão mais vulneráveis a crimes informáticos.

Por terem os filhos em casa, muitos pais podem sentir "uma falsa sensação de segurança". Mas mesmo a partir do seu quarto, os menores podem "passear" à vontade pela internet, e "o mundo cibernauta é tudo menos seguro", alerta.

Com a pandemia de Covid-19, é "impossível dizer que não" às crianças - têm de continuar na internet para acompanhar as aulas e comunicar com os amigos, mas os pais não devem baixar a guarda. O especialista deixa o alerta: "vamos ter muitos casos de crimes sobre crianças. Não tenho dúvidas sobre isso."