O que nos ensina o ciberataque ao governo alemão?

dinheirovivo.pt/opiniao/o-que-nos-ensina-o-ciberataque-ao-governo-alemao-12692524.html

8 de maio de 2020

A Covid-19 continua a ser o mote para ciberataques e o governo da Renânia do Norte-Vestfália, no oeste da Alemanha, foi a mais recente vítima. Embora o valor total esteja ainda sob investigação, estima-se que o prejuízo financeiro possa chegar aos 100 milhões de euros.

O esquema usado foi simples e terrivelmente eficaz: os autores do ataque terão replicado um *website* para requisição de apoios financeiros, no contexto da pandemia, roubado os dados dos requerentes e submetido fraudulentamente os pedidos de apoio. Mal sabia o governo da Renânia que, ao deferir os pedidos e proceder aos pagamentos, estaria a atribuir os subsídios de milhares de queixosos a cibercriminosos.

Em causa estão vários tipos de ataque, como a fraude/burla financeira ou o roubo de identidade, ataques esses que não são novos, mas que têm vindo a crescer significativamente nos últimos meses. O aproveitamento do "fator humano", leia-se de pessoas (e organizações), sobretudo quando se encontram mais vulneráveis, pelas razões que todos conhecemos, é, infelizmente, uma "arte" muito antiga que, com o suporte das novas tecnologias, só ganha mais força.

Este ataque em específico revela, no entanto, algumas particularidades que não devem ser descuradas, especialmente quando sabemos que é tendência cibernética copiar e reproduzir ataques bem-sucedidos. Refiro-me à sua astúcia, sentido de oportunidade e ambição.

Replicar um *website* oficial não é, atualmente, algo particularmente complexo nem moroso. Mas é preciso astúcia e engenho para replicar o site oficial do governo da Renânia - precisamente quando se propõe a apoiar os particulares com um subsídio –, descobrindo o potencial de um único vetor de ataque, encontrando o timing ideal e agindo rapidamente para que a taxa de sucesso, mais uma vez, seja incrementada

Claro está que o sucesso deste ataque está intrinsecamente ligado à ausência de controlos de segurança no que respeita o procedimento – de caráter humano - no decorrer do pedido de apoio.

Não posso deixar de questionar:

- Será que o referido governo alemão fez tudo o que estava ao seu alcance para garantir um procedimento seguro *step-by-step* tendo (também) em atenção a proteção de dados dos seus utilizadores?

- Que outras vulnerabilidades poderíamos encontrar nas várias plataformas digitais associadas a esse governo tendo em consideração as fragilidades – e imaturidade no tema da cibersegurança - detetadas neste ataque?

- Se este ataque fosse replicado no contexto das entidades nacionais públicas e privadas que também atribuem apoios financeiros a particulares ou empresas, no quadro da covid-19, será que seria igualmente bem-sucedido?

Ainda que seja impossível prever um ciberataque, tenho sérias dúvidas sobre a maturidade daquele governo em termos da disciplina de cibersegurança. Afinal, pouco investimento em segurança da informação e iliteracia digital fazem um belo *cocktail* para cibercriminosos poderem desenvolver o seu "ganha-pão" diário.

Para além da componente de segurança preventiva, existem hoje algumas ferramentas preditivas, capazes de emitir alertas e detetar desvios, nomeadamente no âmbito da investigação forense, e que poderiam ter evitado que o ataque em análise se estendesse por aproximadamente um mês, sem que ninguém se apercebesse dele, até que o governo finalmente fosse capaz de detetar o incidente, removesse o referido *site* fraudulento e suspendesse os pagamentos.

Costuma dizer-se, na gíria da cibersegurança, que *n*ão é uma questão de se, mas de quando vai ocorrer um ciberataque. Contudo, a grande mensagem não se prende com o facto de, mais tarde ou mais cedo, todos podermos ser vítimas de um ciberataque, o que nos poderia levar à inércia. O grande "segredo" está, sim, na possibilidade de, através da implementação de medidas de cibersegurança, retardar essa "inevitabilidade" e diminuir o seu impacto.

Bruno Castro é CEO da Visionware