CRÓNICA DO OBEGEF
Nº 70 /2023-08-03
http://www.obegef.pt

Aldo Andretta

> > A Fraude vai acontecer! E o quão rápido as organizações vão agir?

A introdução ao tema que será aqui discutido nesta crônica vem sendo discutido com muita frequência: a capacidade de resiliência das organizações frente a concretização de ameaças cibernéticas, fraudes e lavagem de dinheiro. O motivo é bem simples: aumento de canais que, principalmente as organizações financeiras disponibilizam para facilitar a vida de seus clientes.

Lembro que alguns anos atrás era difícil imaginar que um banco não teria uma agência para irmos abrir uma conta ou fazer uma transação mais complexa. A tecnologia trouxe todas as facilidades possíveis para que a pessoa possa ter o maior conforto possível.

E neste contexto, pensando em fraude, já tínhamos pessoas indo aos bancos com documentos falsos para abrir suas contas bancárias; outras fazendo transações financeiras com o intuito de branqueamento de capital e assim por diante. Nos parece que toda essa facilidade despertou a criatividade de pessoas má intencionadas.

O grande desafio das organizações é conciliar seus interesses e as proteções de seus ativos e clientes. E o como fazer é a grande questão. Muitas tecnologias que contribuem nesta proteção estão surgindo no mercado, mas nem uma delas é a “bala de prata” que resolverá todos os problemas de uma só vez. E as organizações sabem disso!

Para se ter uma ideia desta preocupação, uma empresa que trabalha com tecnologia de proteção, a *BioCatch* encomendou uma pesquisa em os maiores bancos mundiais, sendo que

78% responderam que não conseguem responder de forma eficaz as tentativas de fraude (https://www.biocatch.com/press-release/fraud-and-financial-crime-study).

Essa pesquisa traz alguns pontos interessantes e que levam algumas reflexões. A quantidade mencionada acima de empresa que entendem que não conseguem tratar o assunto de forma eficaz, se deve provavelmente as empresas terem o correto entendimento de que os crimes financeiros aumentam a cada dia, pois 75% dessas tem este pensamento. Na minha humilde concepção os crimes não só aumentam, como principalmente aqueles que acontecem na esfera digital se transformam de maneira muito, mais muito rápida. Quando uma organização consegue ter uma mitigação considerada eficaz, pode acreditar que ela ou vai ser burlada em algum momento ou que vão encontrar um outro ponto de conseguir seu intento.

Ainda a boa notícia trazida pela pesquisa, mostra que 80% das empresas estão se dedicando ao tema e que devem manter a melhor abordagem. Porém, somente 8% delas se sentem à vontade de se manifestar publicamente que oferecem proteção. Tenho o entendimento que este pensamento é correto. Isso pelo motivo de que os fraudadores, muitas vezes não atacam as empresas, mas sim os usuários, pelo motivo que é mais fácil e que tem o que importa: os dados pessoais.

Em outros textos que escrevi sobre este tema, trouxe que uma organização bancária brasileira estava inovando na comunicação, alertando sobre a prática de fraude. Hoje já são três! Pude pesquisar que em Portugal há estudos que relatam que 10% das pessoas que utilizam a internet já sofreram algum tipo de fraude, fazendo com que o Banco de Portugal implemente um programa para uso com maior segurança (https://www.publico.pt/2023/05/10/economia/noticia/quase-10-portugueses-usam-internet-ja-vitima-fraude-financeira-2049081).

A educação é um pilar no combate a fraudes sem dúvida alguma e contribui muito com as empresas nos seus trabalhos, porém é um caminho extremamente longo a ser percorrido e não está totalmente nas mãos das organizações. Já é difícil trabalhar com este tipo de educação digital dentro das organizações, por mais controlos que existam, imagina com um público externo.

E toda essa preocupação demonstrada pelas organizações, reflete a consciência de que as empresas sofreram um ataque cibernético, uma fraude ou qualquer outro ato ilícito a qualquer momento, por mais que invistam em mecanismos preventivos. Isso é um facto! O que

importa hoje é identificar, corrigir e se recuperar de maneira muito rápida, para que os prejuízos sejam menores.

Tal acção só é possível quando há união de diversas áreas dentro das organizações, como o próprio time de negócios, áreas de prevenção a fraudes e cibersegurança, bem como reunir o maior número de ferramentas possíveis para identificar as ameaças e crimes contra a organização. E isso é possível!

Espero ter dado mais um contributo com a disseminação de um tema tão relevante e pode causar diversos prejuízos para todos!