

Fernando Amaral
Chairman
Sendys Group

Black Friday, Natal e cibersegurança

Outubro, a correr para novembro, e eis que vamos a passos largos a caminho da Black Friday, da Cyber Monday, e o tão desejado Natal já se começa a sentir no ar. Um período mágico para milhões de consumidores e para o retalho, que entra na época mais importante do ano. Mas não só. É também o momento de ouro para o cibercrime.

Tal como no eterno 'Sozinho em Casa', milhares de cibercriminosos preparam-se para fazer exatamente o mesmo que os lendários Harry e Marv: aproveitar o frenesim, a avidez e o deslumbre da época para entrar onde não foram convidados. Esta é, com toda a certeza, também para eles, uma época mágica.

Sei que esta não é uma mensagem particularmente natalícia, mas a realidade raramente respeita o espírito da época.

Até final do ano, multiplicam-se campanhas, reforçam-se equipas, afinam-se cadeias logísticas e projetam-se recordes de vendas. Como vimos, há também quem esteja a preparar-se para esta época com igual entusiasmo.

Durante anos, a cibersegurança viveu confortavelmente remetida para os departamentos de IT. Era uma matéria técnica, povoada por acrónimos incompreensíveis e apresentações que, regra geral, só conseguiam competir com maçadora folha de cálculo.

Até ao dia em que a caixa registadora deixa de funcionar. Usando o lugar comum: não é se vai acontecer, é quando. Nesse momento, a cibersegurança deixa de ser um tema tecnológico. Passa a ser um tema operacional, financeiro e reputacional. E, sobretudo, um tema de confiança do consumidor.

Quando uma loja deixa de vender, perde faturação. Quando os sistemas logísticos falham, perdem eficiência. Mas, quando os clientes deixam de confiar, perde-se muito mais do que isso.

Sabemos que a cibersegurança é encarada como um custo, até ao momento em que um ataque paralisa uma operação numa sexta-feira de novembro ou expõe dados de clientes numa das semanas mais importantes do ano. Nessa altura, transforma-se instantaneamente em investimento. E não é difícil perceber porquê.

É nesta época do ano que os atacantes afiam as unhas. Os números não deixam margem para romantismos natalícios. A Fortinet identificou mais de 18 mil domínios associados a campanhas sazonais, como Black Friday, Christmas ou Flash Sale. Destes, milhares foram classificados como maliciosos. Em paralelo, outros milhares de domínios foram criados para imitar marcas conhecidas de comércio eletrónico, funcionando como isco para consumidores e colaboradores menos atentos.

Também a Darktrace fez saber que há um crescimento exponencial das campanhas de phishing dirigidas aos compradores durante a Black Friday, muitas delas recorrendo à impersonação (fazer passar-se por uma marca para cometer um crime) de marcas reconhecidas, para aumentar a credibilidade das mensagens.

A explicação é simples: os atacantes seguem o dinheiro. E, poucas alturas do ano concentram tanto dinheiro, tanta pressão operacional e tanta dependência tecnológica como o último trimestre.

Os retalhistas dependem de uma complexa rede de sistemas interligados. Caixas de pagamento, plataformas de e-commerce, programas de fidelização, aplicações de gestão de stock, centros logísticos e fornecedores externos fazem parte do mesmo ecossistema. Quando um deles falha, o impacto espalha-se rapidamente.

O RH-ISAC, que acompanha o setor do retalho a nível internacional, identifica a Black Friday e a Cyber Monday como períodos particularmente críticos, marcados pelo aumento de tentativas de fraude, ataques automatizados, comprometimento de contas e ações de extorsão.

Mas, existe uma consequência frequentemente subestimada: o dano reputacional. Quando uma cadeia de lojas sofre um ciberataque, a notícia torna-se pública. Quebra a confiança de clientes e parceiros, levanta questões a investidores e coloca os reguladores no encalce. Tudo o que nenhuma marca deseja.

O consumidor pode não compreender a diferença entre ransomware, phishing ou compromisso de credenciais, mas compreende perfeitamente uma coisa: que confiou os seus dados a uma marca e essa confiança foi quebrada.

Se reconstruir sistemas pode demorar dias, recuperar a confiança pode levar anos.

A NCC Group, registou, este ano, um aumento de 50% nos ataques globais de ransomware, com o retalho entre os setores mais impactados, devido à sua elevada dependência operacional e ao valor dos dados que detém.

A questão, por isso, já não é saber se uma cadeia será alvo de uma tentativa de ataque. Será. A questão é perceber se estará preparada para continuar a operar, proteger os seus clientes e preservar a sua reputação quando isso acontecer.

À medida que nos aproximamos da época mais importante do calendário comercial, os líderes do retalho deveriam colocar uma pergunta simples às suas organizações: se amanhã os sistemas parassem, durante quantas horas conseguiríamos manter a confiança dos nossos clientes? Porque, quando a caixa registadora deixa de funcionar, a cibersegurança entra finalmente na agenda dos decisores. E, quando a confiança do consumidor desaparece, já não estamos perante um problema tecnológico. Estamos perante um problema de negócio. Dos grandes.H