Cibersegurança para todos os meses do ano

Bruno Castro
Fundador e CEO da VisionWare – Sistemas de Informação SA

Anualmente, em outubro, assinala-se o mês europeu da cibersegurança. A iniciativa promovida pela Agência Europeia de Cibersegurança (ENISA) com o intuito de alertar para os riscos de segurança de "vivermos" no mundo online e promover boas práticas, completa 10 anos desde que começou a ser assinalada na União Europeia. Uma década depois, estamos (praticamente!) na estaca zero.

Todos os anos, o Mês Europeu da Cibersegurança tem como tema principal, salientar determinadas questões (e problemáticas) no domínio da cibersegurança. O tema deste ano é o ransomware (ou ataque com programas sequestradores) e o phishing, duas grandes tendências constantemente observadas no atual cenário das ciberameaças. E Portugal, infelizmente, não podia ser melhor exemplo face à luz dos acontecimentos cibernéticos desde o início deste ano, a alastrar a diversos setores essenciais da nossa sociedade.

Desde o início de 2022 que temos observado inúmeros ciberataques em praticamente todas as áreas da nossa comunidade, demonstrando que raras são as áreas que escapam à espiral crescente do cibercrime e que nós, enquanto cidadãos e entidades, continuamos mal preparados ao nível da maturidade digital, uma realidade visível em todos os setores.

Precisamente dentro dos setores mais vulneráveis, a Grande Distribuição não é exceção. Sendo esta uma área que envolve diversos stakeholders em simultâneo – consumidores, fornecedores, logística e distribuição – o risco de as cadeias retalhistas serem alvo de ciberataques é elevado, especialmente pela utilização de grandes volumes de informação diversa, com um enorme prejuízo potencial para as entidades, mas também para o cliente final. Acarreta o facto de ser um setor disperso ao nível da cadeia de abastecimento, no sentido em que, cada ponto da cadeia apresenta níveis de segurança díspares (armazéns de logística, empresas de distribuição e transporte, pontos de venda e lojas, e ainda, sedes das organizações).

A melhor forma de manter este tipo de negócio protegido é efetivamente exigente, sendo importante uma avaliação e definição de uma estratégia de proteção e modelo de segurança contínua e transversal. É fundamental não só a prevenção dos dados dos clientes finais assim como a manutenção do controlo e monitorização da interação com os parceiros externos.

Aproveitando assim esta atenção especial ao mês da cibersegurança cabe-me continuar a alertar para os riscos do cibercrime, todos os meses, todos os dias. O facto de termos progredido enquanto sociedade digital e online, não significa que nos devemos esquecer que, tal como nós, também muitos criminosos estão mais 'ligados'. Até porque a prática do crime online permite ao (ciber)criminoso ser mais bem-sucedido pois lucra mais do que no crime tradicional, de maneira mais fácil e é mais difícil ser apanhado.

Desde o início da pandemia, aliás, aproveitando-se da transição digital inesperada e prematura a que muitas organizações foram sujeitas, mas também aliada à falta de resiliência em termos de cibersegurança que já tinham, muitas empresas portuguesas foram e continuam a ser digitalmente "assaltadas" com enormes perdas financeiras, e pior, de dados.

Neste sentido, implementar um conjunto de medidas de cibersegurança permite-nos usufruir deste admirável mundo novo digital. Permite-nos, ainda, crescer e saber responder a um mercado onde a concorrência é cada vez mais apertada e acelerada. Permite-nos responder melhor aos nossos clientes, fidelizá-los, conquistar a sua confiança. Basta reconhecer o problema e querer dar o passo estratégico de colocar o tema da cibersegurança e do seu inevitável investimento, na gestão de topo.

Os ciberataques e a cibercriminalidade continuam a aumentar, em número e em grau de sofisticação, em toda a Europa. Esta tendência deverá acentuar-se no futuro, uma vez que, de acordo com os mais recentes dados divulgados pelo Conselho da União Europeia, se prevê que, até 2024, cerca de 22,3 mil milhões de dispositivos em todo o mundo estarão ligados à Internet das Coisas. Posto isto, não devemos dar especial importância à cibersegurança apenas no mês de outubro, se não, nos restantes 11 meses do ano. **H**