2021: Odisseia no Ciberespaço

dinheirovivo.pt/opiniao/2021-odisseia-no-ciberespaco-14452692.html

31 de dezembro de 2021

No rescaldo desta época festiva, chega a altura do ano em que nos debruçamos sobre aqueles que foram os grandes temas que marcaram 2021, no que diz respeito à segurança da informação.

Com a (continuação) de cenário de pandemia como pano de fundo e o teletrabalho intermitente, optei por trazer ao Dinheiro Vivo temas que marcaram a atualidade nestes últimos 12 meses e que vão, definitivamente, definir o futuro: a inovação dos ciberataques (de acordo com o contínuo dinamismo das ciberameaças), o mundo (ainda) pouco credível das criptomoedas, o aparecimento das cidades inteligentes, a expansão dos serviços "cloud", ou por fim, a força do (ainda recente) conceito dos serviços de intelligence, para nomear apenas alguns exemplos.

Numa altura em que filmes distópicos e futuristas regressam às salas de cinema (e de casa, através de plataformas de streaming - outra realidade, também ela, outrora inimaginável), não consigo evitar questionar-me sobre o quão distantes estamos dos nossos antepassados, que nos trouxeram a ficção científica e um imaginário que prevalece até hoje. O desenvolvimento tecnológico tem vindo a ser cada vez mais extraordinário e o salto que foi dado nas últimas décadas foi abismal (como a chegada da internet a Portugal há 30 anos). Mas, como em todos os maiores desenvolvimentos que temos vivido, há ainda questões que continuam a ser descuradas e erros que são cometidos recorrentemente em todos os "saltos" geracionais, ainda mais, quando o futuro (em particular) - exponencial na sua evolução tecnológica - está repleto de ameaças e riscos para os quais não estamos inteiramente preparados.

Não é por isso de estranhar que, revistas de dimensão global, como a Foreign Affairs, tenham escolhido, dedicar a sua primeira edição de 2022 ao tema da "(Desordem) Digital". É que, neste universo, a que podemos também chamar de ciberespaço, as relações de poder tradicionalmente estabelecidas entre Estados, cidadãos, organizações e o tecido empresarial estão ainda por definir. Indivíduos e grandes estruturas, com as melhores e piores intenções, podem circular livremente nesta "realidade paralela", ao melhor estio "Matrix", sem grandes controlos de fronteira geográfica ou da sua própria identidade. Mais do que circular, podem também agir, com impacto considerável e com um (ainda) certo grau de impunidade.

Como preparar, então, o futuro?

Criar e aplicar regras baseadas nas boas práticas deste novo mundo digital é uma das formas. Veja-se o exemplo de Portugal: foi finalmente publicado o DL 65/2021, de 30 de julho, que regulamenta o Regime Jurídico de Segurança do Ciberespaço - aprovado anos

antes e que transpõe a chamada Diretiva NIS (Network and Information Security) - assegurando a execução das obrigações decorrentes do Cybersecurity Act, do Parlamento e Conselho Europeu, sobre certificação da cibersegurança.

Isto significa que, a Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais e Prestadores de Serviços Digitais têm de adotar um conjunto de medidas, baseadas em análises de riscos prévias, de forma a garantir um nível minimamente robusto de segurança da informação, sob pena de, para além de estarem mais vulneráveis a ciberataques, também poderem sofrer elevadas coimas por não corresponderem ao nível de segurança exigido à sua atividade. Além disso (e, aqui, desde 29 de novembro), têm de ter nomeado um ponto de contacto permanente com o Centro Nacional de Cibersegurança (CNCS), idealmente uma equipa para que seja garantida a disponibilidade e capacidade de resposta 24/7 exigida, e um responsável de segurança que gira as referidas medidas, ambas portanto, diferentes do encarregado de proteção de dados), nomeadamente, junto das Autoridades face a eventuais riscos ou até incidentes de segurança que possam vir a ocorrer nas Instituições/Organizações que representam.

Ou seja, uma boa parcela do tecido empresarial português, a par do Estado, está obrigada (desde 8 de novembro de 2021), a ter um plano formal de segurança e a notificar o CNCS sempre que haja um incidente com impacto relevante ou substancial (conceito por si "perigosamente" abrangente), sob pena de, para além de todo o impacto que possa implicar um ciberataque com sucesso, sofrer, mais uma vez, uma pesada multa junto das respetivas Autoridades de controlo. Acresce ainda, a elaboração de um relatório anual sobre o tema e um inventário sobre todos os ativos essenciais a entregar em conjunto no último dia útil de janeiro do ano civil seguinte. Diria que, face ao recente desafio da implementação do Regulamento Geral de Proteção de Dados, no âmbito do nível de maturidade neste tema da nossa realidade nacional, privada e pública, não é certamente "coisa pouca".

Criar e aplicar regras é apenas uma maneira de planear e orientar os próximos passos na resposta às exigências deste "novo" futuro. Do outro lado, é preciso que as organizações implicadas tenham a capacidade para responder a estas exigências sem condicionar, obviamente, o seu desempenho (já por si) tão crucial para o país.

É aqui que empresas com o histórico da VisionWare, prevendo que este dia chegaria, já entraram há muito tempo no tema da regulamentação de critérios e exigências de cibersegurança, por setor de atividade (banca, seguros, defesa, transportes, etc.). Quando começámos a acompanhar os nossos clientes na definição do plano da segurança da informação, muitos deles desde a nossa fundação, em 2005, disponibilizámos desde logo, um modelo continuado de serviços de consultoria e auditoria nesta matéria, com um objetivo principal: que a organização implementasse um modelo de governação - "vivo" e com o envolvimento obrigatório do top management - de avaliação e melhoria contínua do seu nível de segurança face às exigências, algumas restritivas e complexas, em vigor no seu setor de atividade. Só assim, e com a perspetiva de virem a ser regulados a curto/médio prazo, saberíamos que estariam sempre preparados para qualquer que fosse o modelo de avaliação e regulação estipulado, visto que o "trabalho de casa" já estaria a ser realizado previamente e de forma autónoma (sem a "imposição" das autoridades

regulatórias". A nossa missão era só uma: contribuir para o seu sucesso, aumentando a sua cultura e maturidade em segurança da informação. Hoje, percebemos que esse trabalho em muito facilita a capacidade de resposta às atuais exigências de mercado, aliviando as dores de crescimento que fazem, naturalmente, parte desta existência na atual "desordem digital".

Depois da experiência com o RGPD, que apanhou desprevenidas várias empresas e organizações, levando a inúmeros casos de incumprimento e sucessivas multas, a sua implementação acabou por se transformar num fator de fortalecimento e prevenção da segurança de inúmeras organizações e respetivos destinatários, incrementando a sua credibilidade junto do mercado (apesar da inicial resistência) já que sabemos o quão importante é colocar imediatamente mãos à obra.

Se ainda não colocou a segurança da informação da sua organização na lista para prioridades para 2022, parece-me cada vez mais óbvio que está no momento de repensar a sua estratégia nesta era digital.

A palavra de ordem para 2022 tem de ser "prevenir" e nos cá estaremos para o apoiar!

Boas entradas e até breve!

Bruno Castro, CEO da VisionWare