#AlertaCiberAtaques2022. Quem está a salvo?

jornaleconomico.pt/noticias/alertaciberataques2022-quem-esta-a-salvo-837978

27 de janeiro de 2022

Empresas

Bruno Castro, CEO da VisionWare, especialista em Segurança da Informação, Cibersegurança e Investigação Forense 27 Janeiro 2022, 10:27

Em muitas empresas, o tema da Segurança da Informação e da Cibersegurança já não é encarado como anteriormente, ou até há poucas semanas atrás, como um "custo" demasiado avultado ou até dispensável.

No arranque de 2022 assistimos a uma escalada de ciberataques inéditos por todo o mundo. A 2 de janeiro, vimos com espanto e preocupação, o ataque informático cirúrgico dirigido a um dos maiores grupos editoriais nacionais – a Impresa. Num ciberataque direcionado e sem precedentes no nosso país, o Grupo Impresa encontra-se até hoje, mais de duas semanas após o alerta dado às autoridades competentes, com os seus sistemas informáticos em baixo e com sites provisórios.

Nos últimos dias temos assistido a uma intensificação e sofisticação deste tipo de ciberataques (e crescente clima de ciberterror), com especial incidência na vertente geopolítica/geoestratégica, através do cáustico ciberataque da Rússia ao Governo da Ucrânia, para usurpação de dados relevantes e segredos de Estado.

À medida que os ataques se tornam mais severos e de amplo impacto, as tensões já agudizadas entre os governos afetados pelo crime cibernético e os governos cúmplices da sua atuação aumentam também, ao mesmo tempo que, a cibersegurança se torna mais uma barreira para divergências – em vez de cooperação – entre os Estados-Nação.

Veja-se ainda, e já em Portugal, o desfecho do caso *Russiagate* com a multa singular (e bem avultada) aplicada à Câmara Municipal de Lisboa (CML) no valor de 1,2 milhões de euros, no âmbito da violação da proteção de dados pessoais. Em causa está o facto de a CML ter violado o Regulamento Geral de Proteção de Dados (RGPD) ao "comunicar os

dados pessoais dos promotores de manifestações a entidades terceiras", nomeadamente embaixadas de vários países. Entende a Comissão Nacional da Proteção de Dados que "o arguido Município de Lisboa" violou vários artigos da Lei de Proteção de Dados.

Muito acelerado pela pandemia e pela progressiva persistência da Covid-19 por toda a Europa, existe um *wake up call* para esta tendência e foco na Cibersegurança, que já se afigurava para 2022, mas cujo precipitar de inúmeros ciberataques logo no arranque deste ano, fez lançar o derradeiro alerta aos olhos dos grandes decisores e gestores de topo para este assunto.

Na realidade, os "assuntos informáticos" deixaram de ser uma prioridade e objetivo circunscrito aos responsáveis/CIO dos Departamentos Informáticos das Empresas, Organizações, Entidades e Organismos Públicos diversos.

Assistimos atualmente, e em tempo real, a uma verdadeira transformação do *mindset* da nossa gestão de topo para incorporar o tema da Segurança da Informação e da Cibersegurança como um tópico de investimento prioritário e de proteção do seu bem mais precioso – a Informação –, e já não encarado como anteriormente (ou até há poucas semanas atrás) como um "custo" demasiado avultado ou até dispensável.

No caso específico da VisionWare e desde o caso Impresa, temos sido diariamente solicitados e consultados por CEO, gestores de topo, vereadores e presidentes de Câmaras Municipais, e já não pelo diretor de informática ou responsável pela área de IT das empresas e organizações, qualquer que seja a sua dimensão; solicitam a nossa intervenção imediata e o desenho de um plano estratégico de ação/auditorias específicas aos seus sistemas, com vista à prevenção e proteção máximas da sua Informação.

Ainda no âmbito da mudança de *mindset* (e com necessidade urgente de revisão), um relatório sobre Maturidade Digital em Cibersegurança fornece dados preocupantes: 90% das empresas não têm ainda profissionais especializados em cibersegurança e 82% não mantêm atualizados os registos dos ativos digitais a proteger nas suas organizações. Ao mesmo tempo que cresce a dependência dos sistemas digitais, crescem em paralelo as ameaças à cibersegurança.

Este relatório destaca ainda que, só em 2020, os ataques de *malware* e *ransomware* aumentaram em 358% e 435%, respetivamente, e estão a ultrapassar a capacidade das sociedades de preveni-los ou de responder com eficácia.

Ainda na sequência desta tendência de crescente preocupação e sentimento de qualquer empresa poder ser a "próxima vítima", vimos também a declaração assertiva do nosso Presidente da República Portuguesa que veio a público abordar este tema, dada a criticidade e atualidade mediática do tema. Marcelo Rebelo de Sousa refere que "é preocupante que alguém queira interferir para além das regras do Estado de Direito", acrescentando ainda que, "as intromissões no domínio digital na atividade de órgãos portugueses são verdadeiramente preocupantes e também um reconhecimento do peso da comunicação social".

A pandemia acelerou a transição digital das empresas (e das pessoas), contudo, fez também emergir a grandeza e as repercussões dos ciberataques e expor as fragilidades dos sistemas informáticos. O caso mais recente e por si só mediático do próprio Grupo Impresa, em véspera de eleições legislativas nacionais, tornou-se na face mais visível da galopante preocupação e tentativa apressada (e sem estratégia) de prevenção de novos ciberataques, cada vez mais sofisticados e requintados por grupos de hackers espalhados por todo o mundo.

Urge assim prevenir e colocar a *one million dollar question:* a sua empresa, está a salvo?