Até quando vamos trocar prevenção por improviso?

jornaleconomico.sapo.pt/noticias/ate-quando-vamos-trocar-prevencao-por-improviso

O alerta emitido pelo Serviço de Informações de Segurança (SIS) a 8 de abril de 2026, trata-se de mais um sinal político, económico e estratégico que obriga Portugal a repensar, com urgência, a forma como encara a proteção das suas infraestruturas críticas num contexto internacional cada vez mais hostil e imprevisível.

A operação global atribuída ao grupo APT28, associado ao serviço de informações militar russo (GRU), confirma aquilo que muitos ainda insistem em tratar como hipótese remota: a guerra híbrida já está em curso e o ciberespaço tornou-se um dos seus principais teatros operacionais, marcado de campanhas silenciosas, persistentes e altamente sofisticadas, desenhadas para recolher informação, infiltrar sistemas estratégicos e preparar acessos futuros a ativos críticos.

A utilização de routers domésticos e empresariais como porta de entrada revela precisamente essa lógica. O objetivo não é apenas comprometer um equipamento isolado, mas explorar a infraestrutura digital comum para alcançar redes de maior valor, intercetar comunicações, desviar tráfego e consolidar presença sem levantar suspeitas. É uma abordagem indireta, paciente e adaptada a longo prazo – o que a torna particularmente eficaz.

Portugal não está fora deste tabuleiro de xadrez geopolítico. Pelo contrário, a sua integração em alianças estratégicas, a relevância atlântica, a participação em estruturas da NATO e a presença de ativos sensíveis fazem do país um alvo indireto de elevado interesse. A ideia de que a dimensão reduzida de Portugal o torna irrelevante é, neste contexto, um erro estratégico.

O problema é que a exposição externa cruza-se com fragilidades internas que continuam por resolver. As infraestruturas críticas deixaram de ser apenas barragens, portos, redes elétricas ou hospitais. São também os sistemas digitais que suportam essas operações, os fornecedores que lhes prestam serviços, os dados que circulam entre parceiros e as cadeias tecnológicas que ligam todos esses elementos. A sua segurança depende de um ecossistema inteiro, e não apenas do operador principal.

É precisamente nesse ecossistema que Portugal revela maior vulnerabilidade. A estrutura empresarial portuguesa é composta, em larga medida, por micro, pequenas e médias empresas, muitas delas integradas em cadeias de fornecimento críticas, mas sem recursos adequados para monitorização contínua, resposta a incidentes ou investimento estruturado em cibersegurança. São, frequentemente, o elo mais fraco de redes complexas e, por isso mesmo, o ponto de entrada ideal para atores estatais ou grupos avançados. Empresas incapazes de proteger os seus sistemas tornam-se mais

vulneráveis a interrupções operacionais, perda de dados, danos reputacionais e exclusão de cadeias internacionais cada vez mais exigentes em matéria de segurança.

Os dados internacionais reforçam esta perceção. O relatório Global Cybersecurity Outlook 2026, do World Economic Forum, identifica a geopolítica como o principal fator a moldar estratégias de cibersegurança. Cerca de 64% das organizações afirmam já considerar ciberataques motivados por tensões geopolíticas, incluindo espionagem e disrupção de infraestruturas críticas, enquanto 91% das maiores empresas alteraram as suas estratégias de cibersegurança em resposta à volatilidade internacional. Estes números mostram que o setor empresarial global reconhece o impacto direto do contexto geopolítico na exposição digital. Ignorar esta tendência seria, para Portugal, um luxo que não pode permitir-se.

Portugal precisa, por isso, de uma abordagem mais ambiciosa e integrada. Isso implica investimento consistente em modernização tecnológica, reforço de capacidades de monitorização, desenvolvimento de *risk intelligence* e formação especializada. Implica também que conselhos de administração, gestores públicos e decisores políticos deixem de delegar o risco digital exclusivamente em departamentos técnicos e o assumam como matéria estratégica de governação.

Num cenário internacional em que a competição entre Estados se estende às redes e aos sistemas invisíveis, a proteção das infraestruturas críticas tornou-se uma condição de autonomia e soberania nacional. Até quando vamos improvisar em vez de prevenir?