Covid-19 abriu porta a uma “pandemia cibernauta”

jornaleconomico.sapo.pt/noticias/covid-19-abriu-porta-a-uma-pandemia-cibernauta-724461

11 de abril de 2021

A pandemia da Covid-19 não expôs apenas as fragilidades dos sistemas e dos serviços nacionais de saúde em todo o mundo. Os efeitos sociais e económicos do novo coronavírus também contribuíram para uma maior exposição das organizações (Estado e sector privado) às ameaças do mundo digital. Em Portugal, o último ano “foi inevitavelmente marcado, ao nível da cibersegurança, pela pandemia de Covid-19”, afiança o Relatório Anual de Segurança Interna (RASI) de 2020, divulgado no final de março.

Em declarações ao Jornal Económico, Bruno Castro, o presidente executivo da VisionWare, empresa portuguesa especializada na análise forense de crimes informáticos, afirma que o contexto pandémico “também se traduziu numa pandemia cibernauta”, tendo em conta “um crescendo enorme de ciberataques e de roubos de dados ou de dinheiro”.

De acordo com os dados do RASI, no último ano, “notou-se um considerável aumento do número de incidentes, principalmente a partir do mês de março”, época em que foi declarado o primeiro estado de emergência e em que as empresas iniciaram a transição para regime de teletrabalho. Ao todo, as autoridades portuguesas identificaram 6.525 (+93% face a 2019) incidentes de cibersegurança, dos quais apenas 1.418 foram analisados e resolvidos. Acresce os cerca de 183 milhões de observáveis (alterações discretas num dispositivo ou sistema cujo tratamento é automático), dos quais mais de 61 milhões “encontravam-se relacionados com o ciberespaço nacional”.

Os incidentes encontram-se nas classes fraude, código malicioso, intrusão e segurança da informação (ransomware), sobretudo. O phishing, o SMS phishing e o spearphishing foram os tipos de ataques mais comuns. As ações maliciosas simulavam vir de bancos ou outras instituições de serviços financeiros, serviços do Estado, bem como empresas de logística e de transporte, para obter indevidamente dados ou dinheiro. A estas somam-se as "operações cibernéticas ofensivas" contra o sector da saúde, incluindo ações de ciberespionagem, que procuravam a "exploração de oportunidades no contexto da pandemia".

Mas o crescimento do aumento de ciberataques explica-se como? "A partir do momento em que surge a pandemia, as empresas e o Estado tiveram que dar um salto, na maioria dos casos muito maior que a perna, para o entrar no digital", explica Bruno Castro. O especialista realça que adaptar as operações das empresas ao teletrabalho "foi um desafio tecnológico". Afinal, o trabalho remoto "era uma tendência para daqui a dez anos", não fosse a pandemia.
"A necessidade foi instantânea e foi necessário resolvê-la funcionalmente. Mas, na maioria dos casos, sem garantir a segurança", salienta o CEO da VisionWare.

A par da adoção do teletrabalho, as empresas cujas operações não passavam pelo digital tiveram de adaptar os negócios a um novo mundo. E "fizeram-no rapidamente", mas mais uma vez sem "pensar na segurança".

"Infelizmente, esse hiato entre adotar o teletrabalho ou adaptar os negócios ao digital e pensar na segurança foi demasiado longo e permitiu vários tsunami de ciberataques, que tiveram sucesso", resume o especialista.
Nesse hiato, o sucesso dos ciberataques foi determinado pelo fator humano, visto que, habitualmente, "os ataques são orientados especificamente para um determinado responsável da organização".

O problema da cibersegurança já não pode justificar-se com ignorância das empresas, tendo em conta o mediatismo do tema da cibersegurança, por via de notícias sobre a alegada interferência cibernética nas eleições norte-americanas de 2016, sobre warfare (guerra tecnológica), roubo de dados ou burlas informáticas. "Hoje, quem está nesse nível é por opção", refere Bruno Castro.

Então, o que justifica o crescimento dos ciberataques? A falta de de preparação aliada a uma "imaturidade tecnológica".

Na maior parte dos casos, os problemas terão surgido porque "as empresas não se preocuparam com o tema no passado, não avaliaram o nível de risco – isto é, o nível de maturidade de segurança da empresa". Assim, também "não se prepararam tecnologicamente" e, consequentemente, os trabalhadores "também não estavam preparados para ter de conviver de forma tão agressiva com o mundo digital". "Em contexto de teletrabalho, as pessoas não estão protegidas pela estrutura corporativa da empresa", acrescenta.

Solução passa por avaliação contínua dos riscos e ameaças

Apesar do aumento de ciberataques em Portugal, o país não compara com os "Estados Unidos, Israel, Itália, Espanha ou Inglaterra, que têm outro tipo de propensão a ser atacados". Mas Portugal "já começa a ter um nível de maturidade interessante", tendo em conta que o país avança na transição digital, uma tendência mundial.

Bruno Castro diz que "ainda há um caminho a percorrer, que é longo e tortuoso". Por isso, defende que as organizações devem procurar ter estratégias para a cibersegurança, tentando minimizar a exposição das operações.

Qual é a solução? "Temos que partir do princípio que não existe uma vacina mágica ou um Ferrari das firewall. Para se ter uma maturidade em termos de segurança reativa e preventiva há que avaliar em contínuo as fragilidades e definir soluções caso a caso", explica. Isto para perceber o nível de segurança e criar "um plano de ação para combater fragilidades". "Foi o que faltou em grande escala nesta pandemia cibernética. Quando as organizações eram atacadas nem sabiam por onde eram atacadas", diz.

Para minimizar o risco associado ao fator humano, o especialista diz que "é crítico" apostar na "formação e consciencialização" dos trabalhadores.