E depois da pandemia?

dinheirovivo.pt/opiniao/e-depois-da-pandemia-14188924.html

4 de outubro de 2021

Após quase dois anos de teletrabalho, reuniões remotas, aulas à distância e de um investimento nunca antes visto na forçada transição digital, o mês de outubro, que, curiosamente, é também o mês europeu da cibersegurança, vai marcar, com o fim das restrições, um novo ciclo de recuperação pós-pandemia. Mas regressar à normalidade não pode significar descurar a (ciber)segurança.

Com a pandemia de COVID-19, indivíduos e organizações foram obrigados a saltar quase instantaneamente para o ciberespaço e ali coexistir, enfrentando os riscos e as ameaças cibernéticas deste novo mundo. Foi uma transição dura e abrupta, pelo que não posso deixar de aplaudir a coragem dos gestores de tantas empresas portuguesas - sobretudo, pequenas e médias - que, num período de tempo recorde, as adaptaram à nova realidade. É que, se algumas organizações já tinham, nos vários conceitos (operacionais e funcionais), a maturidade e a experiência do "meio digital", a grande maioria de tecido empresarial ainda o encarava com alguma relutância.

Colocar uma organização online, seja ela privada, pública, pequena, média ou grande, não é uma tarefa fácil, ainda para mais nestes últimos dois anos. Em muitos casos, não havia sequer disponibilidade de tecnologia para construir uma estrutura funcional para os colaboradores trabalharem remotamente ou para continuarem a sua atividade junto dos seus clientes via Internet. Um dos maiores desafios com que nos deparámos foi o de interligar a rede corporativa (e respetivos sistemas) com as múltiplas redes domésticas dos colaboradores que, apesar de estarem em casa, tinham de manter a atividade da empresa. Ou seja, proteger a rede empresarial e, simultaneamente, garantir que também as redes domésticas se interligavam à empresa sem colocar em causa a sua segurança. De uma maneira geral, não havia um nível de literacia digital maduro, que promovesse a sensibilidade para os riscos de estar na Internet, quer para o indivíduo, quer para a organização

Junto das organizações com quem tivemos o privilégio de colaborar durante este período, reconhecemos um grande esforço de investimento humano e financeiro para colocar todas estruturas da empresa a operar com o conceito de teletrabalho, formando colaboradores e testando sistematicamente a segurança. A prioridade foi continuar a atividade empresarial através dos canais de comunicação existentes em cada fase da pandemia.

Algumas organizações já tinham um nível de maturidade de segurança da informação mais avançado do que outras, mais foi quase transversal o esforço realizado no sentido de tentar responder aos desafios que a pandemia trouxe ao mundo dos negócios. Mesmo aquelas empresas que chegaram até nós pela infelicidade de terem sido vítimas de ciberataques bem-sucedidos, com casos extremamente complexos e disruptivos de fraude, roubo financeiro ou de extorsão, tiveram uma abertura inexplicável das camadas de

gestão de topo para elaborar e implementar, quase imediatamente, um plano estruturado de segurança da informação, com um olhar atento ao papel das pessoas, processos e tecnologia, mitigando os impactos do ataque ocorrido, mas tendo em vista a prevenção de ataques futuros.

Tendo isto em mente, é fundamental, nesta nova fase que se inicia, questionar: o que fazer com todo este investimento realizado?

A nossa resposta é simples: não regredir! O mundo mudou, e nunca mais será o mesmo. Como tal, o progresso realizado no setor da segurança não deve ser posto em causa. Pelo contrário, deverá ser mantido ao ponto de fazer evoluir o nível de segurança das empresas para o que agora é exigido. Pois, tal como o mundo mudou, também as exigências no que respeita a cibersegurança mudaram.

Por isso, é essencial continuar a implementar processos e boas práticas, manter a monitorização e a formação dos colaboradores, para solidificar conceitos e treinar a sua sensibilidade para os riscos, mesmo que não estejam a ser considerados sistemas híbridos de trabalho remoto para o futuro próximo. O mindset de segurança já foi criado, portanto basta manter a estratégia.

Podemos afirmar que a pandemia nos colocou à prova, revelando que podemos ter de enfrentar, nos nossos negócios e individualmente, muitos desafios para os quais não estávamos preparados. Melhor, podemos dizer que nós é que colocámos a pandemia (e os seus desafios) à prova, ao responder-lhe com estratégias concertadas de segurança de sucesso, que tornaram as empresas mais resilientes e preparadas para tudo o que ainda há de vir.

Continuemos com o bom trabalho!

Bruno Castro, CEO da VisionWare