Estar na "cloud" garante selo de cibersegurança?

dinheirovivo.pt/opiniao/estar-na-cloud-garante-selo-de-cibersegurança-13892102.html

1 de julho de 2021

O aumento de ciberataques a nível mundial e a fragilidade "digital" resultante das mudanças impostas pela pandemia permitiram o surgimento de novas tendências e oportunidades de negócio, nomeadamente soluções rápidas, eficazes e que ajudam a transmitir segurança a quem as adota. Uma dessas tendências que tem vindo a ganhar notoriedade é a cloud, que, apesar de ser encarada, por muitos, como um recurso infalível, pode implicar mais riscos, caso a estratégia de gestão da sua própria segurança não for garantida.

Mas o que é, afinal, a cloud?

De acordo com a Agência da União Europeia para a Cibersegurança, Cloud Computing é um modelo de serviço on-demand de fornecimento de variadas tecnologias e sistemas de informação, muitas vezes baseado em virtualização, tipicamente assente em infraestruturas tecnológicas e físicas bastante robustas (performance, disponibilidade e eficiência), com uma forte capacidade de computação distribuída. Existem três categorias: **SaaS** - software as a service; **PaaS** - plataform as a service; e **IaaS** - infrastucture as a service.

Embora este serviço seja vendido, para além de tudo o resto, como forma de evitar problemas de segurança, é fundamental desmistificar algumas crenças. Tal como não existe nenhuma solução milagrosa que dê um selo de garantia no que respeita a cibersegurança, também a opção cloud, por si só, não garante a proteção total (ou sequer próximo disso) às organizações. Prova disso é o recente ciberataque à plataforma cloud da NATO, reportado no passado dia 21 de junho, que, alegadamente, terá permitido acesso a informação classificada.

No plano da segurança da informação, nunca se pode prometer risco zero. O que se pode prometer é uma gestão inteligente e dinâmica do risco e, inclusive, do seu eventual impacto, em caso de ocorrência, e isso só é possível através de um trabalho contínuo que considere sempre a tríade pessoas-processos-tecnologia.

Depois, é preciso analisar que, ao adquirir um serviço cloud, junto de um prestador de serviços de mercado, está a abdicar completa ou parcialmente do controlo e gestão da sua própria infraestrutura, pelo que é fundamental que o fornecedor seja fidedigno, certificado e, principalmente, que exista um controlo e envolvimento continuo (através de auditorias, reuniões de controlo, etc.), tal como seria realizado se a transferência não tivesse efetivamente ocorrido. Ou seja, o facto de existir a transferência de ativos da organização para uma entidade externa, não nos desresponsabiliza da obrigação de continuar a manter o controlo quer dos ativos (e informação) em causa, quer da performance e eficácia do fornecedor que decidimos envolver na gestão da nossa infraestrutura.

Por fim, é preciso ter em conta que, a partir do momento em que integramos o ciberespaço, estamos expostos a uma realidade complexa, onde as ameaças se multiplicam, partem de várias frentes e crescem em sofisticação, numa velocidade extremamente difícil de acompanhar.

Tome-se como exemplo uma casa. Sabemos, por senso comum, que não é possível anular completamente a possibilidade de assalto. Então, investimos numa fechadura mais forte. No entanto, sabemos também que esta de nada servirá, se nunca trancarmos a porta, se não tivermos alguns cuidados no que diz respeito à entrada e saída de estranhos ou se, apesar de todos estes cuidados, deixarmos uma janela aberta.

No contexto da cibersegurança, este exemplo ganha outras proporções. As portas de entrada são de maior número e muito menos óbvias. A ameaça pode passar por um equipamento "inteligente", como um alarme ou uma televisão, pode surgir sob a forma de correio eletrónico, download de ficheiros maliciosos ou websites pouco fidedignos e, até, ser provocada pelos habitantes da própria casa, por exemplo através de uma pesquisa inocente, mas desprotegida, feita por um filho ou até por nós próprios.

Quando ganhamos alguma consciência destes perigos cibernéticos, adotamos estratégias e regras que vão para além da aquisição de um excelente computador, antivírus ou serviço de cloud. Criamos passwords complexas, colocamos a informação importante em pastas secretas ou explicamos aos nossos filhos que não devem aceder a determinados sites.

No contexto das empresas, que têm ainda mais atenção a estes temas e, normalmente, equipas internas ou contratadas para gerir e monitorizar a segurança, enquanto colaboradores, somos incentivados a criar passwords complexas e a mudá-las frequentemente, a utilizar acessos remotos seguros (VPNs) para aceder a informação corporativa mais sensível ou a participar em formações, com regularidade, para que nos mantenhamos alerta. Enquanto chefias, contratamos serviços de auditoria para garantir que somos postos a prova e que temos um certo grau de maturidade em segurança que nos legitime juntos dos clientes, assegurando, por exemplo, que a informação confidencial está devidamente protegida.

Ora, se estrategicamente parece mais apelativo optar por uma transposição da infraestrutura para a cloud, é fundamental não descurar no princípio, mantendo a formação, as boas práticas e o controlo contínuo, nomeadamente através de ações de auditoria regulares para identificar e corrigir preventivamente vulnerabilidades, ou até a validação da performance de quem gere a cloud onde passámos a viver. Caso contrário, estaremos a substituir segurança por um golpe de fé e a entregar de olhos fechados a chave de nossa casa.