Os três focos da cibersegurança em teletrabalho: tecnologia, processos e pessoas

hrportugal.sapo.pt/os-tres-focos-da-ciberseguranca-em-teletrabalho-tecnologia-processos-e-pessoas

December 17, 2020

Se ainda existiam dúvidas sobre se o teletrabalho passaria a fazer parte do "novo normal", as mais recentes medidas de combate à pandemia de COVID-19 deixaram-nos esclarecidos: o teletrabalho veio para ficar e negá-lo só faz com que existam descuidos, nomeadamente no plano da cibersegurança.

Por Bruno Castro, CEO da VisionWare

No seio do tecido empresarial, e entre as empresas sujeitas à obrigação de teletrabalho, observamos os seguintes cenários:

· o das organizações que, em Março, já tinham adoptado este modelo e, entre essas, as que já tinham estrutura para isso e as que a tiveram de o criar em "modo instantâneo";

· o das que estão agora a adoptar pela primeira vez este modelo.

No primeiro cenário, a minha recomendação vai no sentido dessas empresas aprenderem com os erros de Março e corrigirem-nos quanto antes. No outro cenário, digo-lhes que procurem fazer uma transição ponderada, sem precipitações, responsável e gradual – adaptada à sua realidade – para que não incorram nos mesmos erros que as restantes.

Resumidamente, isto significa, em termos de cibersegurança, colocar o foco em **três aspectos**:

1. Tecnologia

2. Processos

3. Pessoas

É imperativo garantir que os colaboradores têm a tecnologia necessária para efectuar o seu trabalho. Não se trata apenas de disponibilizar computadores ou telemóveis. Trata-se de garantir que estes equipamentos, que num ambiente de teletrabalho passam a ligar– em modo de "ponte" – as várias redes domésticas dos seus colaboradores à rede corporativa, têm as condições necessárias para um teletrabalho em segurança, para todos os envolvidos. Isto só é possível se os acessos, e o respetivo ambiente "hibrido" entre doméstico e corporativo, forem testados e avaliados com regularidade no que respeita à sua segurança.

Como digo muitas vezes, **a tecnologia, por si só, não é uma solução milagrosa**. É fundamental ter **processos** definidos (por exemplo, direitos de acesso e privilégios) e torná-los mais robustos, para que mitiguem as vulnerabilidades que o teletrabalho acrescenta. Isto implica conhecer o modo de funcionamento da empresa e delinear um conjunto de procedimentos adequados ao seu bom funcionamento. Além da definição e implementação de regras de segurança junto dos colaboradores, sobretudo neste panorama de relação ambígua entre as redes domésticas e a rede corporativa, é importante que as empresas possam monitorizar a sua rede corporativa em "tempo real" de forma a detectar atempadamente eventuais ataques ou comportamentos erróneos/suspeitos que mereçam uma acção reativa de forma a minimizar o seu impacto. É preciso estar ainda mais alerta visto que as ameaças oriundas de redes domésticas podem comprometer a segurança da rede corporativa onde reside o "negócio" das empresas.

Por fim, é absolutamente determinante preparar as **pessoas** da organização. Isto significa consciencializá-las para os riscos e boas práticas a adotar neste contexto tão diferente do corporativo, que é trabalhar de casa. Até porque o factor humano está cada vez mais, e de forma directa, ligado aos incidentes de cibersegurança que têm vindo recorrentemente a ocorrer no tecido empresarial. Este foco é particularmente importante e, felizmente, uma aposta cada vez maior das empresas. As nossas acções de formação e-learning em matéria de cibersegurança, privacidade e segurança da informação têm, aliás, nos últimos meses, cada vez mais procura.

Ou seja, é essencial, que as organizações invistam em tecnologia e auditem continuamente os seus sistemas de forma a conhecer as suas vulnerabilidades, estabeleçam meios de monotorização e alarmística internos, procurem apoio para a implementação/reforço dos seus processos e optem pela formação dos seus colaboradores nestas matérias. Pelo bem de todos!