ATUALIDADE

Teletrabalho motiva aumento substancial do número de ciberataques

O "aumento substancial do número de ciberataques ocorrido nos últimos meses" e a mediatização de alguns casos, nacionais e internacionais, ligados ao cibercrime e à transição forçada para o teletrabalho, têm colocado a cibersegurança na ordem do dia a nível mundial, mas também em Portugal.
Em declarações à 'Vida Económica', Bruno Castro, especialista em cibersegurança e partner da VisionWare, fala sobre a importância de proteger sistemas eletrónicos, computadores, redes e dados contra ataques maliciosos em tempos de pandemia e alerta que os "portugueses não se protegem o suficiente" e têm ainda "alguma dificuldade em perceber e admitir que foram vítimas de um ciberataque".

Cibersegurança não é, nem pode ser, uma preocupação exclusiva do departamento de informática, relembra Bruno Castro.

FERNANDA SILVA TEIXEIRA
fernnadateixeira@vidaeconomica.pt

O crescimento exponencial do teletrabalho, induzido pela situação de pandemia que vivemos, tem aumentado os riscos de ciberataques às empresas. Os mais recentes dados indicam que "houve um aumento substancial do número de ciberataques nos últimos meses, essencialmente pelo próprio contexto de pandemia e porque nem as organizações nem as pessoas estavam preparadas para o teletrabalho", começa por afirmar Bruno Castro.

Segundo explica o partner da VisionWare, por um lado, "aumentaram as burlas e os ataques de roubo de dados e de identidade relacionados com a própria Covid-19, que é ainda um tema atrativo para ataques de "phishing". Por outro, a exposição aos riscos de segurança face à utilização e interligação de redes domésticas e redes empresariais e o facto de os cibercriminosos saberem que as empresas passaram a estar expostas através dos seus funcionários aumentaram o número de ciberataques bem-sucedidos".

Esta mudança foi mais fácil e menos arriscada para as organizações que têm vindo a investir, de forma estruturada e contínua, em cibersegurança, que já tinham testado o conceito de trabalho remoto e que formaram os seus colaboradores para os riscos online nesse mesmo contexto. Ora, no entender deste responsável, tal demonstra que a "cibersegurança não é, nem pode ser, uma preocupação exclusiva do departamento de informática. Este é um aliado fundamental para inserir o tema na "agenda e na estratégia de evolução tecnológica da organização junto dos seus gestores". Porém, a "cibersegurança tem de fazer parte de qualquer estratégia de negócio", sentencia o especialista.

Contudo, reconhece Bruno Castro, não existem soluções milagrosas nem iguais para os vários modelos de negócio que existem. "As necessidades de cada empresa variam consoante o seu nível de maturidade em termos de segurança da informação, os seus objetivos e o orçamento. É preciso analisar continuamente as fragilidades da organização e do seu modelo de negócio, e apoiar os gestores na definição de prioridades sérias, claras e realistas de forma a concretizar um investimento adequado à sua realidade".

Nesse sentido, existem alguns instrumentos públicos em Portugal para ajudar as empresas a fazer face a ciberataques. O Centro Nacional de Cibersegurança e a Agência da União Europeia para a Cibersegurança (ENISA), que são, respetivamente, as autoridades nacional e europeia, em matéria de cibersegurança, têm produzido alguns instrumentos de apoio, em alinhamento com a legislação nacional e europeia sobre o tema.

Há, no entanto, "algum desfasamento entre a necessidade dos instrumentos e a sua disseminação, o que é perfeitamente natural quando estamos a falar de organizações estatais ou paraestatais onde a burocracia é pesada. Mas numa realidade tão dinâmica como a que se vive no ciberespaço, em que aquilo que era verdade hoje já não é amanhã, é determinante estar à frente do nosso tempo. Por isso, as organizações privadas acabam por ter um papel único no que concerne ao desenvolvimento de soluções eficazes e difíceis de igualar", relembra o responsável.

"Portugueses não se protegem o suficiente"

Citando o último relatório do Centro Nacional de Cibersegurança, divulgado em junho deste ano, Bruno Castro indica que as "empresas portuguesas e os próprios cidadãos têm dificuldades em reconhecer que foram alvo de incidentes de cibersegurança e, também, têm menos seguros contra este tipo de incidentes do que cidadãos e empresas de outros países europeus". Ou seja, os "portugueses têm ainda alguma dificuldade em perceber e em admitir que foram vítimas de um ciberataque e não se protegem o suficiente".

Segundo o partner da VisionWare, embora não exista propriamente um barómetro de monitorização do nível de maturidade de cibersegurança nos vários países, há indicadores que comprovam que ainda "existe um desconhecimento dos conceitos básicos de cibercrime e de cibersegurança, o que leva algumas empresas, sobretudo as mais pequenas ou de setores de atividade menos exigentes, a cometerem o erro de não colocar este tema no topo das suas prioridades".

Questionado sobre até que ponto existe ou não uma perceção dos riscos cibernéticos e da importância da sua prevenção, quer no Estado quer nas empresas nacionais, o especialista reconhece que, "nos últimos anos, temos vindo a assistir a um investimento maior na área da cibersegurança, particularmente das grandes empresas, mas também no tecido empresarial das Pequenas e Médias Empresas (PME) e de instituições e organizações governamentais".

Porém, infelizmente, "continuamos a ter gestores e organizações que nunca ouviram falar em cibersegurança até se tornarem vítimas; outros que não lhe dão o devido valor e se limitam a investir em "firewalls" e antivírus, pensando que assim estão seguros e que este tipo de soluções é suficiente. Ou ainda aqueles que julgam que só as grandes empresas ou só algumas empresas de determinados setores é que estão em risco. Obviamente, tudo muda quando são atacados e, nessa altura, passam também a colocar a cibersegurança na ordem do dia, numa perspetiva de prevenção em vez de reação".

Ainda assim, acrescenta, "naturalmente, e cada vez mais, também encontramos organizações que investem em cibersegurança e que estão muito atentas a esta nova realidade em que a segurança informática, tal como a segurança tradicional, é um pilar. Temos sentido isso em relação ao Estado, mas também em alguns setores de mercado e em algumas empresas de pequena e média dimensão, onde a cibersegurança, associada à privacidade, passou a ser obrigatória".

Nesse contexto, o responsável salienta ainda que, embora exista uma estratégia nacional, pelo menos no que concerne aos organismos públicos, pois existem determinados instrumentos jurídicos que obrigam ao cumprimento de um conjunto de requisitos mínimos de segurança, o grande desafio está em perceber que a "cibersegurança só é atingível na sua plenitude se implementada por todos". Ou seja, "posso investir bastante em sistemas tecnológicos para proteger a minha organização e continuar bastante exposto a riscos se não educar os meus colaboradores para as boas práticas de cibersegurança. Posso fazer um grande esforço corporativo para certificar a minha empresa em determinado standard europeu de segurança da informação e estar altamente desajustado da realidade e, até, desprotegido, se não renovar e não fizer uma revisão regular dos preceitos daqueles instrumentos. E posso investir em tudo – certificação, formação, tecnologia – mas tenho de testar, testar, testar! Porque, se não testar, como sei se não fui já atacado?", remata Bruno Castro.

É fundamental "não subestimar" a importância da cibersegurança

A pedido da 'Vida Económica', Bruno Castro, especialista em cibersegurança e partner da VisionWare, deixa alguns conselhos para as empresas nacionais que pretendem reforçar a segurança das suas redes e dos seus dados.
Desde logo, afirma o especialista, é fundamental "não subestimar" a importância da cibersegurança. "Cada minuto que passa online expõe-no a novos riscos. Cada novo equipamento que adquire e liga à rede, seja na empresa, seja em sua casa, pode estar a expor a sua vida e o seu negócio. Estar 'online' é cada vez mais um requisito para a manutenção e sobrevivência do tecido empresarial. Mas, para isso, tem de aceitar que esta nova realidade implica também um tipo de segurança próprio, para evitar dissabores a curto prazo".
Por isso, se for vítima de um incidente de cibersegurança, "denuncie ou peça ajuda a uma empresa de cibersegurança. A verdade é que muitos incidentes podem ser evitados através da implementação de boas práticas, mas, ao mesmo tempo, há outros que são cometidos mesmo por quem tem enorme sensibilidade para a temática", pois os ciberataques são cada vez mais sofisticados e difíceis de detetar, mesmo por especialistas.
Por fim, "invista em cibersegurança e não deixe o seu negócio, e mesmo a sua vida pessoal – que muitas vezes se mistura, nomeadamente em casos de extorsão e chantagem – à mercê de cibercriminosos e/ou da concorrência ou ex-colaboradores insatisfeitos".