A segurança em primeiro lugar
Safety first

Pedro Gaspar
Managing Director
ALIDATA

Fotos cedidas pela empresa
Photos assigned by the company

O momento que vivemos é, sem dúvida, o de maior incerteza das nossas vidas. Mas há uma certeza absoluta que emerge da pandemia: o mundo mudou. E mudou, deixando-nos já duas diretrizes: temos de estar preparados para o inesperado e a segurança vem sempre em primeiro lugar. É assim que, nas tecnologias da informação, desde sempre, pensamos a cibersegurança. Acautelamos o pior cenário, esperando o melhor.

De forma breve, e sem ser alarmista, um quarto das empresas nacionais já foram alvo de um ciberataque, a cada minuto, quase 250 computadores são infetados com malware, e apenas 30 por cento das empresas tem um plano de contingência para o caso de ser alvo de um ataque cibernético. Mas que forma pode ter este tipo de ataque?

Há os conhecidos malware, ransomware e phishing, mas também os ataques internos e a preocupante espionagem industrial, que, em sectores como o mobiliário, deverão ser particularmente acautelados.

A sua empresa está preparada para cada uma dessas ameaças? O malware invade, danifica ou incapacita terminais, sistemas e redes, assumindo o controlo das operações de um dispositivo. O ransomware infecta computadores e servidores, exigindo o pagamento de resgate para voltar a aceder à informação. O phishing recolhe dados confidenciais, através de sites fraudulentos.

Se todas estas ameaças são preocupantes, também a espionagem industrial e os ataques internos, através do acesso a informação confidencial das empresas, por colaboradores ou ex-colaboradores, podem representar graves prejuízos imediatos em projetos em desenvolvimento, mas também reputacionais no mercado e junto de clientes.

Tal como a pandemia nos está a ensinar, não há cenários impensáveis, muito menos improváveis. A segurança dos dados da sua empresa e dos seus clientes é, provavelmente, um dos maiores ativos intangíveis que possui.

The moment we live in is undoubtedly the most uncertain of our lives. But there is an absolute certainty that emerges from the pandemic: the world has changed. And it has changed, leaving us with two guidelines: we have to be prepared for the unexpected and safety always comes first. That is how, in information technologies, we have always thought of cybersecurity. We guard the worst case scenario, hoping for the best.

Briefly, and without being an alarmist, a quarter of national companies have been attacked, every minute almost 250 computers are infected with malware, and only 30 percent of companies have a contingency plan in case of ciberattack. But what form can this type of attack take?

There are the well-known malware, ransomware and phishing, but also the internal attacks and the worrying industrial espionage, which, in sectors such as furniture, should be particularly guarded.

Is your company prepared for each of these threats? Malware invades, damages or disables terminals, systems and networks, taking control of a device's operations. Ransomware infects computers and servers, requiring a ransom payment to access information again. Phishing collects confidential data through fraudulent websites.

If all these threats are worrying, industrial espionage and internal attacks, through access to confidential company information, by employees or ex-employees, can represent serious immediate damage in projects under development, but also reputational in the market and in the customers.

As the pandemic is teaching us, there are no unthinkable scenarios, let alone unlikely. The security of your company's data and that of your customers is probably one of the biggest intangible assets you have.-