Foto: DR

A Cibersegurança na internacionalização das empresas

Cybersecurity and Business Internationalisation

Nelson Escravana
Diretor da Área de Cibersegurança
INOV – Instituto de Engenharia de Sistemas e Computadores, Inovação
Head of Cybersecurity
INOV – Instituto de Engenharia de Sistemas e Computadores, Inovação

O complexo ambiente virtual resultante da emergência da internet, das pessoas e organizações que a utilizam e de todas as atividades, no diverso tipo de dispositivos e redes de comunicações a que designamos por ciberespaço, é hoje um espaço fundamental para o desenvolvimento da atividade económica.

As ameaças decorrentes das vulnerabilidades nos Sistemas de Informação, dos seus utilizadores e da capacidade e motivação para as explorar pelo cibercrime organizado, cujo impacto económico atualmente já se estima o triplo daquele atribuído ao tráfego de estupefacientes, representando mais de 1% do PIB mundial[1], devem ser tomadas em consideração à medida que as empresas transitam para o digital.

No contexto da internacionalização, a transição para o digital é inevitável, quer através da simples ligação à internet, quer através de suportes como o *website* e redes sociais, compras e vendas *online*, relacionamento eletrónico com a Administração Pública, a automatização das linhas de produção, a interconexão eletrónica automática com clientes e fornecedores, a faturação eletrónica e a incorporação no negócio de novos paradigmas tecnológicos como a Inteligência Artificial, o 5G ou a Internet das Coisas (IoT). No entanto, todo este movimento de digitalização aumenta a exposição das empresas a ataques cibernéticos (a chamada superfície de ataque), a qual conjugada com as crescentes ameaças cibernéticas atuais possui o potencial de causar sérios danos, não apenas financeiros e jurídicos, mas também reputacionais. Adicionalmente, a regulamentação europeia de proteção de dados pessoais[2], atribui responsabilidades às empresas, e aos seus órgãos de gestão, na

The complexities of the virtual environment, brought on by the emergence of the internet, the people and organisations that use it, and all the activities, on all different types of devices and communication networks that we collectively refer to as cyberspace, is now a crucial space for the development of economic activities.

The threats that arise from the vulnerabilities of IT systems, their users, and the ability and drive to exploit them on the part of organised cybercrime, which is estimated to move three times more money at the moment than drug trafficking, accounting for 1% of world GDP[1], must be taken into account as companies go digital.

In the context of internationalisation, transitioning to digital is inevitable, by simply being connected to the internet, or through platforms such as websites and social media, e-commerce, an online relationship with civil service, automated manufacturing, automatic online connections with clients and suppliers, online invoicing, and the incorporation of new technological paradigms into business, such as Artificial Intelligence, 5G, or the Internet of Things. However, all this digital movement leaves companies exposed to cyberattacks (the so-called attack surface), which together with growing current cyberattacks has the potential to cause serious damage at the economic, legal, and reputational levels. Additionally, European data protection regulations hold companies, and their management, accountable for protecting the personal data they process, particularly that of their staff, clients, and partners, breaches of which can lead to hefty fines and even to criminal responsibility.

Ransomware, attacks in which a company's data are

1- "The Cybersecurity 202: Global losses from cybercrime skyrocketed to nearly $1 trillion in 2020, new report find", *TheWashingnto Post*, 2020/12/07.
2- Regulamento Geral de Proteção de Dados - REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016.

"Para se preparar para a internacionalização e o mundo digital global (...) uma empresa deve apostar não apenas na constante atualização dos seus Sistemas de Informação, bem como em planos de continuidade de negócio, mas principalmente na consciencialização e formação dos seus colaboradores para lidarem com as ciberameaças. "

"In order to prepare for internationalisation and the global digital world, (...), a company should not only invest in keeping its IT systems and business continuity plans up to date, but should mainly work on raising awareness among their staff, and train them to deal with cyberthreats."

proteção dos dados pessoais que processam, nomeadamente aqueles dos seus colaboradores, clientes e parceiros, podendo resultar em coimas avultadas para além da eventual responsabilidade criminal.

O *Ransomware*, ataque que consiste no sequestro dos dados das empresas, solicitando avultados valores de resgate sem qualquer garantia de recuperação dos dados, foi identificado pela Agência Europeia de Cibersegurança[3] como a principal ameaça em 2021 e merece especial atenção por parte das empresas. Mas a fraude por *e-mail* e muitos outros cibercrimes assolam cada vez mais as empresas que atuam no mercado global.

Apesar de diariamente serem descobertas novas vulnerabilidades que afetam os Sistemas de Informação, obrigando as empresas a manterem os seus sistemas constantemente atualizados, não são estas o principal fator de sucesso para um ciberataque, logo o principal risco que as empresas enfrentam no digital. O fator de sucesso para a larga maioria dos ciberataques, são os utilizadores[4] e a forma como estes lidam com as ciberameaças.

Para se preparar para a internacionalização e o mundo digital global que é hoje um atrativo domínio para os negócios, potenciando o acesso a mercados com uma dimensão largamente superior à tradicional, uma empresa deve apostar não apenas na constante atualização dos seus Sistemas de Informação, bem como em planos de continuidade de negócio, mas principalmente na consciencialização e formação dos seus colaboradores para lidarem com as ciberameaças.

O Polo de Europeu de Inovação Digital em Cibersegurança, C-Hub[5], coordenado pelo Centro Nacional de Cibersegurança (CNCS), disponibilizará a partir de outubro de 2022, um conjunto de serviços às empresas e entidades da Administração Pública, no âmbito da cibersegurança, nomeadamente na experimentação e teste de tecnologias digitais na fase prévia à decisão de investimento, na qualificação e formação em competências digitais, no apoio à procura de financiamento para investimento em tecnologias digitais e atuando como facilitador, juntando indústria, empresas e entidades da Administração Pública.

sequestered, and are only returned after a ransom is paid, was identified by the European Cybersecurity Agency[3] as the main threat in 2021 and deserves special attention on the part of companies. However, e-mail fraud and many other cybercrimes are increasingly becoming a scourge for companies in the global market.

Despite the daily discovery of new vulnerabilities that affect IT systems, forcing companies to keep their systems constantly up to date, these are not the main factors that enable cyberattacks, and therefore they are not the main threat for companies in the digital sphere. The main vulnerability is, in fact, users[4], and the way they handle with cyberthreats.

In order to prepare for internationalisation and the global digital world, which is currently an attractive domain for businesses, giving them large-scale access to markets which are several times larger than the traditional one, a company should not only invest in keeping its IT systems and business continuity plans up to date, but should mainly work on raising awareness among their staff, and train them to deal with cyberthreats.

The European Cybersecurity Digital Innovation Hub, C-Hub[5], which is coordinated by the National Cybersecurity Centre (CNCS), will be providing a series of services to companies and civil service entities, as of October 2022, in the field of Cybersecurity, namely in testing and experimenting with digital technology in the phase before investments, in qualification and training in digital skills, in supporting the search for funding of digital technologies and acting as a broker between industry, companies, and civil service entities.

3- ENISA Threat Landscape 2021.
4- O "erro" humano é fator decisivo entre 60% a 90% dos ciberataques. | Human "error" is the decisive factor in between 60% and 90% of cyberattacks.
5- https://www.c-hub.pt/