Elisabete Maciel

> > Cibersegurança: 2022 *annus horribilis*

Ao longo de 2022, têm sido noticiados numerosos ataques informáticos, alguns deles de consequências muito gravosas (destruição de toda a informação de forma irreversível). O que podemos esperar daqui para a frente?

O CERT.PT (*Computer Emergency Responde Team*), do Centro Nacional de Cibersegurança (CNCS), registou um aumento de 26% de ciberataques em 2021 em Portugal face ao período homólogo. Mesmo que ainda não seja possível indicar uma estimativa para 2022, tudo aponta que a situação vai-se agravar. Basta recordar o que se passou desde o início do ano: mais de uma dezena de ataques a grandes empresas e organismos públicos divulgados pela imprensa - Grupo Impresa, Vodafone, SONAE, Lusa, Parlamento, EMGFA, TAP, Hospital Garcia da Horta, entre outros.

Nessas notícias em concreto, não são abordadas as Pequenas e Médias Empresas (PME), as quais representam cerca de 99% do tecido empresarial português. Será que estas empresas estão livres de ataques? Com certeza que não. Eventualmente, as notícias referentes aos ciberataques a PMEs não são tão impactantes ou assombrosas. Uma certeza nós temos: as PMEs são bastante mais vulneráveis que as empresas de grande dimensão, pois o orçamento disponível para a Cibersegurança, a existir, representa uma percentagem bem mais diminuta do que o das grandes empresas.

Um dos fatores que mais contribuiu para a proliferação de ataques informáticos tem que ver com o trabalho remoto, ao qual foi necessário recorrer massivamente aquando da pandemia. O teletrabalho implicou que os colaboradores pudessem aceder à rede da empresa a partir de qualquer lugar. Frequentemente, uma falsa sensação de segurança dos colaboradores não reforçando a sua segurança online (não atualizar o antivírus, não atualizar o browser, clicar em links suspeitos, não confirmar se os sites acedidos são seguros, etc) foi uma potencial causa de

um ciberataque. Ricardo Marques, *Head of Consulting* na S21 parece confirmá-lo quando defende que "os colaboradores são o elo mais fraco da Cibersegurança e a porta de entrada para a grande maioria dos ciberataques, logo é imperativo que as empresas tenham consciência dessa realidade".

É importante referir que mesmo as empresas que investem significativamente na sua cibersegurança, são ainda assim sujeitas a ataques, e por vezes até bem-sucedidos. Não há empresa que seja inatacável e inviolável. No entanto, verifica-se uma grande distância entre aquelas que se capacitam e as que não o fazem.

Como afirma, e bem, António Gameiro Marques, Diretor Geral do Gabinete Nacional de Segurança, "Há uma diferenciação significativamente positiva entre entidades que tendo sido atacadas recuperaram num tempo finito e recuperaram o negócio… Essa é uma das lições que se tiram dos acontecimentos deste ano.".

Ademais, se atendermos ao Relatório Cibersegurança em Portugal - Riscos e Conflitos elaborado pelo CNCS, podemos verificar que em "2022 e 2023 são identificadas como principais tendências em Portugal a propensão para uma maior intervenção de atores estatais, a persistência do uso das fragilidades do fator humano, ataques de *ransomware*[i], violações de dados relativas a credenciais de acesso, exploração de vulnerabilidades e as tecnologias móveis a serem cada vez mais utilizadas como superfícies de ataque."

As empresas têm de tentar estar um passo à frente de quem as ataca, pois apenas assim conseguirão evitar ou atenuar, eventualmente, as consequências de um ciberataque.

Não se enganem: eles irão continuar; cada vez mais sofisticados e frequentes.

Algumas palavras para as PMEs: esta luta é desigual. Devem apostar na cooperação e nos esforços partilhados, quer seja dentro das associações do setor quer seja a nível municipal, equacionando a criação de um centro de prevenção do cibercrime partilhado.

[i] ***Ransomware*:** tipo de *software* malicioso que permite que um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes. Para a recuperação dos ficheiros, é exigido ao proprietário um resgate monetário.