

Cibersegurança: a palavra do ano

 dinheirovivo.pt/opiniao/ciberseguranca-a-palavra-do-ano--15563388.html

29 de dezembro de 2022

O ano de 2022 foi certamente um dos mais significativos e marcantes para o setor da cibersegurança em termos de evolução da capacidade destrutiva dos ciberataques, do crescimento abrupto do cibercrime, da própria aprendizagem para todos os envolvidos no setor, e do nível de mediatização pública do tema. Se, por um lado, os cidadãos ganharam uma maior consciencialização para a necessidade de proteger os seus dados e toda a sua atividade na Internet face a todos os ataques cibernéticos que ocorreram em diversos setores ao longo deste ano, por outro lado, perceberam a impotência em que se podem encontrar quando estamos perante estratégias cibernéticas que afetam diretamente as sociedades atuais.

Refiro-me, em primeira instância, ao conflito russo-ucraniano, um dos primeiros casos internacionais flagrantes a acontecer em matéria de ciberataques neste ano. De forma a contextualizar os leitores, registou-se um crescimento de 112% de ciberataques a visar o governo e o setor militar ucraniano, assim como, por semana, um crescimento de 1500 ciberataques em empresas ucranianas de diversos setores. A situação agrava-se quando, e para demonstrar a impotência acima referida que os cidadãos podem sentir em caso de um ataque cibernético, são atacados os setores energéticos ou os sistemas de saúde de um país, falando então de ciberterrorismo. A nível nacional, um dos maiores incidentes informáticos a envolver uma entidade estatal ocorreu com o Estado-General das Forças Armadas, após a exposição de vários documentos de teor confidencial enviados pela NATO ao nosso país. Contudo, e numa postura positiva, realço que Portugal tem seguido uma trajetória concordante com as diretrizes que se devem adotar em matéria de cibersegurança, como é o caso da aprovação da Estratégia Nacional de Ciberdefesa no passado mês de outubro.

A privacidade dos dados foi igualmente um dos tópicos predominantes na agenda deste ano. Assistimos a inúmeros ciberataques que afetaram diretamente a esfera pessoal de inúmeros cidadãos - recordemos os ciberataques à Vodafone, TAP, Segurança Social, clínicas Germano de Sousa, Hospital Garcia da Horta, Sonae MC, Grupo Impresa, Agência Lusa, entre outros. A utilização de serviços digitais na Internet, até de forma legítima, promove a divulgação dos nossos dados pessoais em plataformas que muitas vezes desconhecemos o seu nível de segurança, sendo que podemos, ingenuamente, correr o risco de disponibilizar os nossos dados à comunidade cibercriminosa para fins fraudulentos e maliciosos, prejudicando não só a sociedade como um todo, mas também a confiança dos consumidores nestes serviços e no mundo digital de uma forma genérica.

O tema cibersegurança ganhou uma particular mediatização nos meios de comunicação social devido a todos os ataques informáticos decorridos este ano em Portugal, nomeadamente aqueles que foram de tal forma destrutivos que colocaram em causa serviços que sempre julgamos ser fiáveis e seguros. Abalou inclusive o nosso sentido de

confiança no mundo cibernético e nas próprias "marcas" de renome internacional que, afinal, também são vulneráveis a ciberataques. Se, por um lado, é bastante benéfico que a comunidade - profissional e acadêmica - de cibersegurança alerte publicamente para alguns comportamentos de risco que possam ocorrer neste novo paradigma cibernético, por outro lado, assiste-se ao aparecimento de inúmeros supostos "especialistas de cibersegurança" que disseminam vários termos ou "discussões filosóficas" relacionados com a segurança de informação de forma pouco correta. Tendem ainda para as chamadas "teorias da conspiração" que, ao invés de propagar conhecimento sobre o tema, proliferam campanhas de desinformação, sem qualquer rigor ou experiência de causa.

Cabe-nos a todos - cidadãos, empresas, organizações, Estado - prepararmo-nos para aumentar o nosso grau de maturidade digital, tendo sempre como perspectiva o também incremento da nossa capacidade de resiliência para 2023. A Informação tem-se revelado como uma das fontes mais valiosas na comunidade cibercriminosa e, face ao ecossistema digital em que estamos cada vez mais inseridos, prevê-se que o número de ciberataques aumente consideravelmente tal como o seu grau de complexidade, independentemente do setor de atividade ou dimensão da empresa. Urge assim adotar em 2023, uma posição mais responsável, preventiva, resiliente e segura perante a transformação constante que este novo mundo digital nos tem vindo a trazer.

Subscrever newsletter

Subscreva a nossa newsletter e tenha as notícias no seu e-mail todos os dias

Boas Festas e Feliz Ano Novo 2023!

CEO da Visionware