

O caminho inadiável da Segurança e da Privacidade Digital dos Portugueses

 dinheirovivo.pt/opiniao/o-caminho-inadiavel-da-seguranca-e-da-privacidade-digital-dos-portugueses-17079157.html

26 de setembro de 2023

Há uma questão que me é colocada várias vezes: como estão os portugueses relativamente à sua segurança e privacidade digital? A resposta pode não ser tão simples ou consensual, no entanto, o que temos vindo a reparar é que, de facto, existe hoje uma maior noção e conhecimento sobre segurança e privacidade digital, seja por parte do cidadão comum ou das empresas; ainda assim, a base dessa maior consciencialização ainda carece de um foco e aposta essencial muito simples: a formação.

Vamos a exemplos práticos: estudos recentes indicam que Portugal obteve o terceiro lugar do pódio no Resultado do Teste Nacional de Privacidade; à margem deste excelente resultado está a percentagem de portugueses que sabe lidar com ataques de phishing, o qual tem aumentado de ano para ano, passando de 51% em 2021 para 63% em 2023, lembrando que este tipo de ataque é um dos mais comuns em Portugal e, por essa razão, é muito positivo perceber que existe cada vez maior consciencialização e sensibilização para estas temáticas e, sobretudo, como saber agir quando se sofre um ataque deste tipo.

Desde os tempos vividos na pandemia em 2020 e 2021 que temos vindo a perceber que os portugueses consideram importante e necessário estarem seguros no mundo digital, compreendendo melhor os riscos que os rodeiam, como, por exemplo, o simples ato de colocar os dados do cartão de crédito numa página da internet ou lidar com ofertas valiosas (e suspeitas) que habitualmente surgem na internet. E, por isso, passaram a tomar medidas para se protegerem, como criar uma password forte e complexa ou adicionar mecanismos adicionais de autenticação (como o multifator), bem como ter mais atenção ao conteúdo que partilham nas suas redes sociais.

Apesar desta melhor e mais atenta noção de segurança e privacidade digital, os portugueses ainda se mostram preocupados com algumas questões, tais como: de que forma é realizada a recolha de metadados, como proteger as redes Wi-Fi domésticas, qual a importância da leitura dos termos e condições online, e por último, as questões de privacidade e segurança nos seus próprios dispositivos. Começa finalmente a existir consciência sobre a insegurança e as ameaças que existem no mundo cibernético.

Portugal está no top 10 dos países que mais sofreram ataques de ransomware só no primeiro mês de 2023 e foi precisamente este o alerta lançado pela VisionWare, em fevereiro passado, de acordo com dados divulgados através do DarkFeed/DeepWeb Intelligence Feed, 2023 Top Targeted Countries. Estes mostram que o nosso país ficou em 7º lugar, numa altura em que se assinalava precisamente o primeiro ano pós o grave

ciberataque infligido à Vodafone. Aliás, o ataque por ransomware constitui, por isso, uma ameaça visível para milhares de organizações e empresas, a par das tentativas de phishing, inclusive em Portugal, quando comparada com a tendência noutros países europeus.

O que podemos fazer para continuar a subir nos rankings de conhecimento de segurança e privacidade? A resposta é simples: investir na formação, na crescente literacia digital e, sobretudo, na literacia em cibersegurança. Através da VisionWare Academy, área dedicada à formação, com diversos cursos que abordam as distintas vertentes da Segurança da Informação e da Privacidade e Proteção de Dados, auxiliamos e sensibilizamos os nossos clientes, de forma contínua, a alcançarem uma maior maturidade cibernética, nomeadamente, na capacitação de consciência de segurança na convivência no mundo cibernético, ações que se têm revelado bem-sucedidas e com retorno evidente para a segurança global das organizações em geral.

Em relação a estas, para além da formação nesta área em específico, é necessária cada vez mais a capacidade de monitorização constante da segurança, ou seja, além de recursos especializados e bem formados, é necessário estarmos constantemente atentos a possíveis ataques, num conceito de 24 horas x 7 dias, sendo a prevenção a melhor forma e o caminho certo para responder de forma eficaz em caso de ciberataque. Poderíamos também acrescentar a necessidade de criarmos um modelo que permita stressar continuamente os mecanismos de segurança em vigor, através de processos "personalizados" de auditoria. Só assim conseguimos detetar em tempo útil as nossas fragilidades, e por inerência, garantir a sua correção atempada.

Os portugueses têm demonstrado que estão num bom caminho no que toca à segurança e privacidade digital, contudo, não nos podemos desleixar, já que, apesar das melhorias visíveis, não nos podemos esquecer que o fator humano é, normalmente, a maior fragilidade; é crítico continuar a investir em formação e prevenção, porque só assim seremos cidadãos ciber-seguros e ciber-atentos, tornando as empresas mais seguras e "blindadas" a ciberataques.

A aposta é simples: formar, independentemente da função ou cargo, porque qualquer um de nós pode ser vítima de um ataque malicioso ou fraudulento, justamente quando estamos menos atentos ou preparados, e esse é um caminho inadiável e sem retorno.