

O que fazer para prevenir o futuro?

 lidermagazine.sapo.pt/o-que-fazer-para-prevenir-o-futuro

7 de novembro de 2023



[Home](#) › [Opiniões](#) › O que fazer para prevenir o futuro?

Opiniões

7 Novembro, 2023 | 3 minutos de leitura

Manter a desconfiança costuma ser, habitualmente, o melhor caminho a seguir para garantirmos uma maior segurança quando navegamos na Internet e nas nossas redes sociais. Tal como em qualquer esquema fraudulento, devemos manter-nos sempre atentos, preventivos, e sobretudo, não clicar em links cujas origens não conhecemos ou poderão ser de índole duvidosa e/ ou criminosas. Por norma, devemos desconfiar, sempre.

Os ciberataques de ransomware continuam em ascensão, afetando transversalmente todas as áreas de atividade. Devido ao incremento (e manutenção) do trabalho remoto, motivado e acelerado pela pandemia, estima-se que estes ataques tenham aumentado 148% em todo o Mundo. O ransomware constitui, por isso, uma ameaça visível para milhares de organizações e empresas, inclusive em Portugal, que, quando comparada com a tendência

noutros países europeus, e de acordo com dados recolhidos pelo Tech Monitor, surge a ocupar o 3.º lugar com uma incidência de 9% no que toca aos ciberataques registados em toda a Europa no ano 2022. Os protagonistas deste tipo de ciberataques sabem que o seu modelo de negócio, altamente destrutivo, terá garantia de sucesso contínuo, desde que consigam inovar as suas técnicas de exploração e formatos de dispersão dentro da organização.

Há que fazer mais e melhor para prevenir o futuro, já que as implicações e consequências para qualquer empresa e marca podem ser devastadoras (incluindo, por vezes, quando falamos de casos de ransomware violentos e que minam todo o sistema, por exemplo, de uma PME), podendo levar à própria falência de uma empresa e à extinção de uma marca; tal pode ser o cenário devastador e as consequências catastróficas de um ciberataque de sucesso. O ambiente de teletrabalho promoveu um certo descuido face às medidas de segurança, o que faz com que todos, mesmo os mais formados, estejam “menos alerta” para eventuais ameaças ou comportamentos suspeitos. Os níveis de maturidade de segurança variam de organização para organização, mas o fator humano é normalmente a maior fragilidade. As pessoas precisam de ser formadas para responderem a esta nova realidade e poderem novamente conviver com o mundo cibernauta, com tudo o que acarreta, de forma ponderada e responsável. Mais do que literacia digital, há a necessidade de haver literacia em cibersegurança.

É necessário prevenir e investir em modelos de segurança contínuos, conhecer bem as infraestruturas, e sobretudo, “stressar” os sistemas, procurando falhas e fragilidades, corrigindo-as de forma perseverante, de modo a “blindar” a organização contra quaisquer eventuais tentativas de ataques. Em simultâneo, e através de tecnologia, procedimentos, mas também através de testes de stress, deve testar-se vezes sem conta a nossa capacidade de recuperação a um incidente de segurança que possa implicar desastre global na organização. Conhecer a nossa capacidade de recuperação a um ciberataque é hoje fundamental para a gestão de qualquer empresa ou organização de modo a garantir a sua sobrevivência.

Este artigo foi publicado na edição de outono da revista Líder. [Subscreva a Líder aqui.](#)

Bruno Castro,
Fundador & CEO da VisionWare