

## VisionWare promove “Conversas Seguras” sobre a atualidade do IT e cibersegurança

IT [itsecurity.pt/news/analysis/visionware-promove-conversas-seguras-sobre-a-atualidade-do-it-e-ciberseguranca](https://itsecurity.pt/news/analysis/visionware-promove-conversas-seguras-sobre-a-atualidade-do-it-e-ciberseguranca)



A VisionWare promoveu esta quarta-feira as “**Manhãs VisionWare – Conversas Seguras**”, um pequeno-almoço com jornalistas que incentivou o debate sobre alguns dos mais urgentes e emergentes temas relacionados com a **cibersegurança** e o **setor de IT**, em particular no contexto português.

Entre outros, a conversa suscitou a discussão sobre tópicos como o estado de maturidade digital e de cibersegurança em território nacional face ao mundo, sobre estratégias de resposta a ciberataques, as atuais ameaças e desafios, em particular no âmbito da nova economia de cibercrime e do complexo contexto geopolítico, e o VisionWare Threat Intelligence Center.

Bruno Castro, CEO e fundador da empresa, que esteve presente para dinamizar as “Conversas Seguras”, começou por discutir o nível de literacia digital em Portugal, que, apesar de ter vindo a melhorar, ainda se revela baixo. Esta falta de consciencialização para o funcionamento do universo digital e dos respetivos perigos tem sido altamente aproveitada pelos cibercriminosos para direcionarem ameaças. Porque “*estamos mais vulneráveis*” do que no nunca no digital e porque o fator humano ainda é um dos principais vetores de ataque, o cibercrime não para de crescer.

A discussão virou-se para a mais-valia que é a comunicação no contexto do cibercrime, tanto na necessidade de as organizações terem a comunicação de crises embebida na sua estratégia, como da comunicação social na consciencialização da população, das empresas e organizações para os perigos atuais.

O CEO da VisionWare, que se começou a interessar pelo mundo cibernético desde tenra idade devido ao filme WarGames e ao seu pai, engenheiro e professor universitário, explicou que na eventualidade de um ciberataque, a equipa forense tem a última palavra. Assim, enquanto a investigação não estiver concluída, o lado técnico não pode avançar e colocar os sistemas em funcionamento.

Bruno Castro ressaltou, também, a importância de não ceder ao pagamento de resgates, acima de tudo por ser uma demonstração de fraqueza. Segundo explicou, a um ciberataque segue-se um período em que vários cibercriminosos tentam aproveitar as eventuais vulnerabilidades da organização em questão. Além disso, se a organização fizer o pagamento do resgate, mais aliciante se torna.

Entre as maiores tendências no mundo da cibersegurança, o líder destacou os seguros – sobre os quais se demonstra cético –, os testes de recuperação de ataques, e uma forte demanda por SOC. Finalmente, alertou para o grande problema de recursos humanos que a área enfrenta. “*Nas universidades são aprendidas as ferramentas, mas dar o salto para o real demora anos*”, afirmou Bruno Castro. Além disso, “*mesmo formando, a retenção é um problema*”. No caso português, em particular, a dificuldade de retenção agrava-se porque apesar da formação ser de qualidade, há oportunidades mais aliciantes no exterior, em empresas estrangeiras que têm mais capacidade de compensação e melhores condições para oferecer.

[VisionWare Cibersegurança Cibercrime Talento](#)

---