Ciberguerra preocupa 62% das empresas portuguesas

Estudo mundial revela a postura de profissionais de TI dos vários setores face à ameaça de uma ciberguerra

LISBOA, PORTUGAL, January 24, 2023 /EINPresswire.com/ -- O panorama de ciberameaças é cada vez mais complexo, os ataques mais frequentes, sofisticados e severos e a possibilidade de uma ciberguerra cada vez mais real. Porém, apesar dos acontecimentos globais e contínuos mais recentes, como a pandemia e a guerra da Ucrânia, 38% das empresas em Portugal ainda não estão a levar a ameaça de ciberguerra a sério e 37% não estão preparadas para lidar com um evento destes, de acordo com um estudo desenvolvido pela Armis, empresa líder em visibilidade e segurança de ativos, sobre o Estado da Ciberguerra.

Segundo o inquérito, que envolveu mais de 6 mil profissionais de TI, de diferentes setores, em 14 países, 62% das organizações portuguesas estão preocupadas com o impacto de uma ciberguerra na sua empresa, 78% dos inquiridos consideram provável um aumento do orçamento para cibersegurança e 31% afirmaram ter experienciado mais atividade ameaçadora na sua rede. Apenas 53% dos profissionais estão confiantes de que o Governo nacional pode defender-se contra a ciberguerra.

“A ciberguerra é o futuro do terrorismo sob o efeito de esteroides, proporcionando um método de ataque económico e assimétrico, que requer vigilância constante e despesas para se defender", disse Nadir Izrael, CTO e Co-fundador na Armis. "A ciberguerra clandestina está a tornar-se rapidamente uma coisa do passado. Atualmente, já assistimos a ciberataques descarados dos Estados-nação, muitas vezes com a intenção de recolher informações, interromper as operações ou destruir completamente os dados. Com base nestas tendências, todas as organizações devem considerar-se possíveis alvos de ataques de ciberguerra e proteger os seus ativos em conformidade".

Vesku Turtia, diretor regional da Armis na Península Ibérica, explica: “A atual instabilidade geopolítica, associada à invasão russa da Ucrânia, também acelerou o aumento dos ciberataques. Alguns sectores, fundamentais para a economia e sociedade, como os cuidados de saúde, as infraestruturas críticas e o setor industrial, estão particularmente em risco e é primordial que todos sejam protegidos.”

“As organizações portuguesas, que ainda se encontram num processo de transformação e

adaptação aos novos modelos de trabalho remoto e híbrido, terão de investir em cibersegurança para garantir que a adoção de novas tecnologias possa ser feita de forma segura", conclui.

As principais conclusões do estudo da Armis sobre o Estado da Ciberguerra são:
-Em Portugal, 62% das organizações estão preocupadas com o impacto de uma ciberguerra na sua empresa como um todo. Contudo, 38% das empresas portuguesas ainda não estão a levar esta ameaça a sério e 37% acreditam que a sua empresa está pouco preparada para lidar com uma ameaça de ciberguerra, um valor superior à média europeia e global (26% e 24%, respetivamente).
- A atual situação geopolítica aumentou as preocupações sobre uma possível ciberguerra, com 67% dos inquiridos portugueses a concordarem que a guerra na Ucrânia criou uma ameaça maior, ligeiramente acima das médias europeias e globais (63% e 64%, respetivamente). Entre os profissionais de TI inquiridos, 31% afirmaram ter tido uma maior atividade ameaçadora na sua rede entre maio e outubro de 2022, em comparação com os seis meses anteriores. Um valor acima da média europeia (25%), mas igual ao registado a nível mundial (31%).
- Apesar da crescente preocupação com a ciberguerra, as empresas portuguesas continuam concentradas na sua transformação digital. Apenas 35% dos profissionais informáticos portugueses inquiridos pela Armis afirmam que a sua organização parou temporariamente ou abandonou estes projetos, um número significativamente inferior à média europeia (50%) e global (55%).
- Os elementos de segurança prioritários para os profissionais de TI portugueses são a proteção de dados (78% das respostas), a deteção de intrusão (55%) e a gestão de identidade e de acesso (52%). Quanto às ferramentas ou serviços de cibersegurança em que as suas organizações aumentaram o investimento nos últimos seis meses, os inquiridos indicam o Configuration Management Database (46%), seguido da gestão de acesso (45%) e de vulnerabilidade (41%). As principais práticas de cibersegurança implementadas nas organizações são o backup de dados (65%), a utilização de firewall e software anti-malware (64%), e dados encriptados (57%).
- A formação tem sido outro foco das empresas portuguesas. Questionados sobre se a sua empresa realiza formação regular para todos os colaboradores sobre como se comportar de forma segura online, 77% dos profissionais de TI concordaram.
Tendo em consideração os acontecimentos recentes, como a pandemia e a guerra na Ucrânia, 78% dos portugueses inquiridos consideram provável que a sua organização invista mais do seu orçamento em cibersegurança. Atualmente, uma grande proporção das empresas portuguesas apenas atribui entre 5 e 10% do seu orçamento de TI à cibersegurança (41%).
- Quando questionados se confiam na capacidade de defesa do Governo contra a ciberguerra, 53% dos profissionais de TI e segurança portugueses manifestaram-se confiantes. O estudo da Armis também inclui duas questões específicas para o mercado português, relativas ao novo Regime Jurídico para a Segurança do Ciberespaço em Portugal. Quando questionados se o novo regime mudou a forma como as empresas lidam com as medidas de cibersegurança, 53% dos profissionais de TI e de segurança portugueses responderam afirmativamente. À pergunta se as empresas devem ser multadas se não tiverem planos de segurança contra ciberataques, 67% dos inquiridos responderam 'sim'.

- Os resultados do relatório Estado da Ciberguerra e Tendências da Armis: 2022-2023 demonstram a crescente preocupação das organizações com a crescente frequência e severidade dos ciberataques, bem como a ameaça da ciberguerra. O cenário de ameaças cada vez mais complexo e sofisticado está a ter impacto em diversas áreas de negócios, em todas as indústrias. Contudo, ainda há um ritmo e prioridades diferentes na elaboração e adoção de estratégias de cibersegurança.

Mais informações sobre o estudo aqui: www.armis.com/cyberwarfare

para Armis
Adding Value
armis@addingvalue.pt
Visit us on social media:
Twitter
LinkedIn
