Jogos Olímpicos e cibersegurança: que a...

lidermagazine.sapo.pt/jogos-olimpicos-e-ciberseguranca-que-ameacas-se-esperam

14 de junho de 2024

Jogos Olímpicos e cibersegurança: que ameaças se esperam?

Os **Jogos Olímpicos 2024 começam a 26 de julho** e Paris será a cidade anfitriã do maior evento desportivo do planeta que até ao dia 11 de agosto vai receber mais de 10 mil atletas, entre 48 modalidades.

O momento é particularmente vulnerável, não só em virtude do contexto geopolítico, mas também porque **tudo será digitalizado**, logo suscetível à cibercriminalidade.

No que diz respeito a riscos cibernéticos, as previsões apontam para cerca de **3,5 mil milhões de ocorrências de ciberataques no contexto do evento**. Os dados são revelados no relatório da VisionWare, elaborado pelo Threat Intelligence Center.

Principais ameaças

Entre as operações cibernéticas que podem visar os Jogos Olímpicos (JO), destacam-se:

- Campanhas de desestabilização, através de campanhas de influência, *malware* e extorsão de dados, e as campanhas de perturbação, incluindo ataques DDoS e de desinformação. Os ataques de desestabilização são normalmente realizados para fins de ativismo e representam uma ameaça crescente;
- Apesar de não representarem uma grande ameaça operacional, os crimes cibernéticos com vista à obtenção de lucro, são o tipo de ataque que mais frequentemente afeta espectadores, patrocinadores e entidades e indústrias associadas aos Jogos.;
- Operações cibernéticas patrocinadas por Estados, normalmente associadas a tensões geopolíticas que afetam os países anfitriões e os países participantes e têm em vista a recolha de informações ou a sabotagem e perturbação do evento.

Contexto geopolítico

Considerando o atual contexto geopolítico, marcado pelo conflito Rússia-Ucrânia e Israel-Hamas, segundo o relatório, é provável que os JO de Paris sejam alvo de ciber-operações como medida de retaliação. A Rússia foi proibida de competir devido ao sistema de dopagem patrocinado pelo Estado em Sochi 2014 e à invasão da Ucrânia em 2022, o que a coloca como um dos principais atores a observar.

Adicionalmente, o contexto político francês também não deve ser desconsiderado. À semelhança do que aconteceu no Rio de Janeiro em 2016, a atenção dos meios de comunicação social pode ser aproveitada por grupos *hacktivistas*.

Entre os principais atores Estatais a considerar, aponta-se a Rússia, o Irão e o Azerbaijão, e entre os atores não-Estatais destacam-se os grupos *hacktivistas* e cibercriminosos. Entre as vítimas poderão estar os atletas, as agências e peritos antidopagem, os turistas e espectadores, e os patrocinadores e negócios associados aos Jogos.

Por sua vez, a própria infraestrutura dos JO também poderá ser alvo de ciberataques, perturbando os sistemas de venda de bilhetes, as comunicações ou a transmissão. Segundo a análise, as infraestruturas críticas – energia, transportes e recintos olímpicos – são também alvos vulneráveis, uma vez que um ataque bem-sucedido poderá perturbar significativamente, ou mesmo, encerrar o evento.