Going for gold: Security learnings for the Tokyo 2020 Olympics

23/12/2019

Most fans did not have the dream ending they hoped for in this year's Rugby World Cup however, one country was a clear winner. While South Africa took home the trophy, another country was triumphant for its defensive strategy – Japan.

The Japanese players may have performed well on the field, but the nation had even greater success off the pitch by managing to host six weeks of an action packed, high profile championship without suffering a single successful cyber attack.

In previous years, high-profile sporting events, such as the Rugby World Cup, have been a hot-spot for cybersecurity threats, attracting malicious actors looking to capitalise on large gatherings of people and technology as a means to execute various cyber attacks. This ranges from cyber criminals stealing personally identifiable information (PII), or harvesting user credentials for financial gain, to the nation states looking to embarrass the host country.

Now, with 2020 just around the corner, we are less than a year away from the Summer Olympics where Japan will again be in the spotlight as the host of a global sporting event. So, what has the nation learned to ensure the Games' avoid a potentially disastrous cyber attack?

Learnings for cyber resiliency

The 2018 Winter Olympics in Pyeongchang is one example from which the Japanese government and the International Olympic Committee (IOC) will have learned from.

The XXIII Winter Games were so high profile that authorities were on high alert monitoring for possible cyber incidents and related disruptions. Yet, despite this, they were not able to prevent a major cyber attack from taking place ahead of the opening ceremony, which was a cause for international embarrassment.

Hit by an attack dubbed ‘The Olympic Destroyer’, the official PyeongChang 2018 website, which was providing access information and tickets for the event, stopped working. While authorities managed to bring the website back online around twelve hours later, at approximately the same time, the Wi-Fi network at the Olympic stadium, along with TVs and internet services located at the main press centre and other minor systems, also stopped.

While this shut down didn’t cause any major, long-lasting disruptions, the embarrassment caused to the host nation was visible. The opening ceremony is the most-followed event of the Olympic Games and a well-coordinated cyber attack occurring during this time window has a good chance of maximising impact and the related embarrassment.

Steps for a safe 2020

The smooth running Rugby World Cup might have been a testing ground for the defensive strategies of this technologically savvy nation, but there is a lot to be done to ensure a cyber-secure Olympics in Tokyo, which will have a global audience many orders of magnitude larger.

The first step is for the IOC (International Olympic Committee) to ensure every third party organisation involved in the planning and execution of the Games has secure systems. Supply chains and partner organisations have notoriously been the weak link in previous cyber attacks, leading to bigger and more well-known organisations falling victim. Alongside this, researchers from McAfee’s Advanced Threat Research team have previously identified an implant – dubbed Gold Dragon – which has been used to target organisations associated with and involved in the Olympic Games. It’s an implant which could potentially be used again, this time to devastating effect.

As well as this, we know there are cyber espionage groups in the wild which need to be monitored and managed. Fancy Bear (also known as APT28) is one such group, already having been caught performing cyber attacks against, at least, sixteen national and international sporting and anti-doping organisations across three continents.

But how can these groups be kept at bay?

Intelligence is the key to providing effective defence. Understanding the motive of a threat actor or adversary can provide answers and insight to not only stop a threat altogether, but also to help organisations to prepare for similar attacks in the future – the IOC and Japanese government will need as much intelligence as they can gather.

Threat intelligence is just the first step and not only monitors new and old threats, but also speeds up the triage process, should someone attack. By gathering raw data about emerging threats and improving intelligence collection and exploitation, the IOC will be better placed to obtain pre-emptive intelligence on the intent and capabilities of its adversaries than in any

previous Games.

Understanding the bigger picture beyond the impact of the attack itself is critical if we are going to triumph over bad actors. Despite this, intelligence isn't a silver bullet. It is a key piece of a wider puzzle which the IOC needs to put together to have the best defence against an Olympic-sized cyberattack.