Try to tackle cybersecurity during #RWC2019

By Simon McCullough

20 Sep 2019

Get the braaivleis and biltong ready because this year's highly anticipated Rugby World Cup in Japan will be the biggest and most tech-enabled event the world has ever seen.

Simon McCullough, major channel account manager at F5 Networks

From 20 September 2019, 1,8 million tickets will change hands and 400,000 rugby fans will descend on the Land of the Rising Sun to watch their teams scrum, tackle and drop kick their way to victory.

Online activity will also be off the charts.

In 2015, there were over 270 million social media video views, 2,8 million official app downloads, and the #RWC2015 hashtag appeared twice a second. Expect records to tumble again this year as cybercriminals get match fit to breach the security defences of organisers, sponsors and fans alike.

Catching fans (and employers) offside

The 2018 football world cup might have been played with a different shaped ball, but it was also a great lure for cybercriminals and serves as a good barometer for what we may encounter in Japan.

During the football world cup, tactics like phishing and social engineering were widely used to scam unwary fans out of money. We expect this year's rugby world cup in Japan to be no different.

Even in the build-up to the event, fans have been bombarded by a wide range of scams using tournament branding to look legitimate. These include fake apps, betting scams, counterfeit tickets, as well as browser attacks targeting credit card details. Meanwhile, thousands of illegal streaming sites are sitting on the bench waiting for proceedings to start.

With so much excitement in the air, fans may not be paying attention to some of the online red flags. This could pose a problem for businesses. How many employees will place an unsecured bet? How many will attempt to win tickets from a fraudulent website using BYOD or an office-supplied device?

To avoid falling victim to cybercrime:

- Limit public Wi-Fi use or use a private network or virtual private network (VPN) with data encryption capabilities
- Ensure devices have the latest operating system and patches installed
- Question messages with links or attachments - a trusted brand wouldn't immediately ask for personal data or financial information
- Use trusted websites with the HTTPS prefix and avoid search engine-assisted e-commerce spelling mistakes and design flaws are obvious warning signs, but they are getting harder to spot
- Only download apps from trusted sources

IoT mauls

In March 2018, an Interpol conference identified the Internet of Things (IoT) as a major sporting event risk. At the same time, thingbots (such as Mirai) are being harnessed by hackers in greater numbers than ever to form powerful botnets of networked things.

Japan knows the score. Earlier this year, the country's National Institute of Information and Communications Technology (NICT) planned a sweep of around 200 million devices to check for vulnerabilities in connected "things" like routers, webcams and home appliances. It is a much-needed initiative.

Historically, IoT devices tend to prioritise access convenience over security, and the world cup is a timely prompt for widespread awareness and action.

There are no silver bullets of course, and any organisation touching IoT must constantly assess its defensive posture. To combat the thingbot threat, McCullough recommends tackling the most damaging offensive moves first.

For DDoS attacks, that means a cloud scrubbing provider is the way to go. Next up are application attacks, which require specialised application firewalls with behaviour-based bot detection and traffic inspection.

Never cut corners with IoT. Don't buy products with known vulnerabilities, obvious exploit histories or substandard security mechanisms. Quarantine or retire any devices that cannot be secured.

Other IoT exploit path must-dos include:

- Disabling remote management. Restrict operations to a management network, or place behind a firewall. Leverage NAT at a minimum if the devices will be used in a residence.
- Changing vendor default credentials and disabling the default admin account.

- Continually updating devices with the latest firmware as it is released.

Nation-state rucks

The RAND Corporation believes the Tokyo Olympics' biggest cybersecurity threat comes from foreign intelligence services ("should they choose to act"). The same applies to the rugby world cup.

The Verizon Data Breach Investigations Report (VDBIR) recently reported a sharp uptick in nation-state attacks, rising from 12% of all analysed breaches to 23% in the past year.

In another alarming trend, hackers acting on behalf of nation-states are also carrying out more zero-day attacks, which take place on the same day a weakness or vulnerability is discovered.

As the influence of IoT and 5G gets louder and louder, it is important to note that hackers acting on behalf of nation-states are no longer just out to disrupt critical infrastructures – they're also actively seeking business and trade secrets. This means it is critical to have adequate defences that can detect unknown attacks and correctly identify malicious app connections.

Fortunately, a range of new technologies are available for selection. For example, AI solutions can analyse traffic in real-time to spot unusual behaviours and anomalies previously out of sight.

However, there will always be a need to apply security at every level and on every surface: endpoint, application, and infrastructure. Remember, applications require consistent, intelligent and adaptable policies wherever they reside (on-premises, in the cloud or in a multi-cloud environment). Protecting perimeters is no longer enough.

Whatever happens at the rugby world cup, it will be intriguing to monitor cybercriminal activity in the coming weeks. By all accounts, Japan is well prepared, and the tournament could even yield the protective blueprint for future events of this scale. Dropping the ball is certainly not an option – especially with the 2020 Tokyo Olympics also on the horizon.

For the first time ever, rugby fans will be able to watch the world cup through multiple feeds in multiple formats. The organisers have even incorporated Augmented Reality (AR) graphics into the coverage.

ABOUT SIMON MCCULLOUGH

Major Channel Account Manager at F5 Networks
- Try to tackle cybersecurity during #RWC2019 - 20 Sep 2019
- Stay safe from cybercrime with what's left of 2019 - 30 Aug 2019
- Multi-cloud's new multiculturism - 21 Aug 2019
- A new phase of cyber warfare has begun - 7 Aug 2019
- The ABC of DevOps - 27 Jun 2019

View my profile and articles...