STORMSHIELD

MEINUNGEN

CYBERSICHERHEIT UND OLYMPISCHE SPIELE: ERFAHRUNGSBERICHTE VOR PARIS 2024

Victor Poitevin
Editorial & Digital Manager, Stormshield

Die Olympischen und Paralympischen Sommerspiele in Paris 2024 sind die größte Veranstaltung, die seit 1900 in Frankreich stattfindet. Denn die Zahlen können einen schwindlig machen: 7 Milliarden Euro Budget, 4 Milliarden Fernsehzuschauer, 12 Millionen Zuschauer, 30.000 Freiwillige, 10.000 Athleten, 206 Nationen, 40 zu sichernde Wettkampfstätten... Aber auch die, die mit dem Thema Cyber zusammenhängen, dürfen nicht vergessen werden: Nach einer halben Milliarde Angriffen 2016 in Rio war von mehr als... vier Milliarden Cyberangriffen während der Spiele 2021 in Tokio die Rede. Daher die Bedeutung der Cybersicherheit bei diesem globalen Ereignis.

Aus aktuellem Anlass haben die Vorfälle beim Finale der Fußball-Champions-League 2022 in Paris die Grenzen des Umgangs mit physischen Vorfällen aufgezeigt. In Kombination mit der Cyber-Frage und potenziellen IT-Zwischenfällen gehen sie so weit, dass sie die Fähigkeit, die Olympischen Spiele 2024 auszurichten, in Frage stellen. Aber wie bereitet sich Frankreich dann auf die Organisation eines solchen Ereignisses vor? **Welche Cybersicherheit für Paris 2024?** Welche Maßnahmen werden ergriffen, um mit Cyberangriffen umzugehen und sich vor ihnen zu schützen?

WELCHE CYBERRISIKEN BESTEHEN FÜR DIE OLYMPISCHEN SPIELE?

Bei einem solchen globalen Treffen können (und haben sich bereits materialisiert) Cyberangriffe in verschiedenen Formen auftreten. Phishing, Spoofing, Denial of Service (DDoS), Abfangen von Wifi/4G/5G-Streams, Kompromittierung von Geldautomaten ... die Angriffsvektoren sind zahlreich. **Vincent Riou**, Partner bei Avisa Partners, zuständig für Cybersicherheitsaktivitäten und Mitverfasser eines Strategiepapiers zu diesem Thema, geht auf die Attraktivität der Olympischen Spiele für Cyberkriminelle ein. *„Die Olympischen Spiele bedeuten für das Gastgeberland das Äquivalent der Ausrichtung von etwa 60 Weltmeisterschaften zur gleichen Zeit. Sie sind also ein gewaltiger Imageträger für das Land, in dem sie stattfinden, mit Milliarden von Fernsehzuschauern. Das bedeutet aber auch, dass jede noch so kleine Beeinträchtigung an den gesamten Planeten weitergeleitet wird."* **Die Olympischen Spiele ziehen verschiedene Arten von Cyberkriminellen mit unterschiedlichen Motiven an. Karim Benslimane,** Leiter der Abteilung Cyber Intelligence bei Darktrace, beschrieb auf einer Keynote in Lille (Frankreich) im Jahr 2022 eine dreifache Cyberbedrohung: *„An erster Stelle haben wir staatsnahe Cyberterroristengruppen, die geopolitisch motiviert sind und das Ziel haben, das Land zu destabilisieren. An zweiter Stelle haben wir opportunistische, merkantilistische Cyberkriminelle, die durch den Geldsegen in Versuchung geführt werden. Sie setzen beispielsweise auf die Dringlichkeit, mit der die Organisatoren die Situation wiederherstellen müssen, um sie dazu zu bringen, so schnell wie möglich Lösegeld zu zahlen. Und drittens schließlich gibt es Hacktivistengruppen mit ideologischen und militanten Ansprüchen, die Angriffe wie Website-Defacements oder Denial-of-Service durchführen können."*

> *„Die Olympischen Spiele bedeuten für das Gastgeberland das Äquivalent der Ausrichtung von etwa 60 Weltmeisterschaften zur gleichen Zeit. Sie sind also ein gewaltiger Imageträger für das Land, in dem sie stattfinden, mit Milliarden von Fernsehzuschauern. Das bedeutet aber auch, dass jede noch so kleine Beeinträchtigung an den gesamten Planeten weitergeleitet wird."*
>
> **Vincent Riou,** Partner bei Avisa Partners – zuständig für Cybersicherheitsaktivitäten

Für die Organisatoren dieser außergewöhnlichen Veranstaltung sind die Cyberrisiken allgegenwärtig. Videoerfassung für das Fernsehen oder die Schiedsrichter, Videoüberwachungskameras und Alarmanlagen, Ausweis- und Ticketleser ... jedes angeschlossene Gerät ist ein potenzielles Einfallstor für Cyberkriminelle. Hinzu kommen die Logistik und die Zuliefererkette, die die Angriffsfläche erheblich vergrößern. Darüber hinaus integriert diese Pariser Ausgabe Sportveranstaltungen inmitten der Juwelen des französischen Kulturerbes und nicht nur in geschlossenen Stadien. Bogenschießen im Dôme des Invalides, Beachvolleyball am Fuße des Eiffelturms, Fechten im Grand Palais, Eröffnungsfeier auf der Seine ... Diese offenen Orte in der Hauptstadt bringen ihre eigenen Schwierigkeiten bei der Sicherung mit sich. Vincent Riou meint: *„Die Olympischen Spiele an symbolträchtigen Orten in der Stadt auszutragen, ist für die Zuschauer absolut genial.*

Aber diese zu sichern, ist sehr komplex! Wenn Zuschauermassen entlang des Seine-Ufers stehen, stellen Sie sich die verschiedenen Zugangspunkte vor. Wie kann man das alles sichern? Videoüberwachungskameras, Zugangsportale, Datenbanken, um anhand der Ausweise zu sehen, wer eintreten darf und wer nicht. Fernsehübertragungen ... alles ist digitalisiert und damit anfällig für potenzielle Angriffe." Die zunehmende Digitalisierung und Dematerialisierung lässt daher erwarten, dass **das Niveau der Cyberrisiken für Organisatoren steigt**.

Auch Fans, Zuschauer oder Fernsehzuschauer sind hier potenzielle Opfer, indem sie die Auswirkungen von Cyberangriffen zu spüren bekommen, die z. B. zu Ausfällen der Fernsehübertragungen führen. **Nicolas Caproni**, Head of Threat & Detection Research (TDR) Team bei SEKOIA.IO, erläutert: „*Sie können aber auch direkte Ziele von Cyberangriffen sein, etwa im Rahmen von Phishing-Kampagnen: „Opportunistisch werden Cyberkriminelle das Ereignis nutzen, um Phishing-Kampagnen zu versenden, wobei sie sich auf Gewinnspiele stützen, um die Wahrscheinlichkeit zu erhöhen, dass die Nachrichten geöffnet werden und auf kompromittierende Links geklickt wird. Sie können auch im Rahmen von Ticketverkaufs- oder -weiterverkaufsbetrügereien Malware in einer pdf verstecken. Sie werden auch versuchen, an persönliche Daten und Kreditkartendaten zu gelangen, die später im Darknet einen Wert haben.*" Eine weitere Bedrohung wird ebenfalls in Betracht gezogen, nämlich die Verbreitung falscher Informationen. „*Einige Gruppen von Angreifern spezialisieren sich mittlerweile auf Desinformation und Fake News. Diese neuen Waffen können eingesetzt werden, um Veranstaltungen zu stören, indem Daten, die nicht hätten geleakt werden dürfen, oder gefälschte Daten durchsickern. Aufgrund der Komplexität der Umsetzung handelt es sich in diesem Fall meist um staatliche Angriffe.*"

Schließlich sind auch Sportler von Bedrohungen während der Olympischen und Paralympischen Spiele betroffen. Vincent Riou nennt einige Beispiele für mögliche Angriffe auf Athleten: „*Die Zugangsschlüssel zu den Hotels, die Klimaanlage, der Feueralarm, die digitale Anzeige der Spielstände, die Stoppuhren ... alles ist digitalisiert. Stellen Sie sich die Folgen einer Störung der Kühlkette für die Ernährung vor, die auf bestimmte Delegationen abzielt, oder die Aktivierung von Feueralarmen in den Hotels bestimmter Sportler am Vorabend eines wichtigen Wettkampfs.*"

Organisatoren, Zuschauer, Fans und Sportler – ausnahmslos alle sind von den Cyberrisiken bei den Olympischen Spielen betroffen.

EIN JAHRZEHNT DER CYBERANGRIFFE AUF DIE OLYMPISCHEN SPIELE

Die Frage der Cybersicherheit bei den Olympischen und Paralympischen Spielen stellt sich seit etwa zehn Jahren. Bei den Spielen 2004 in Athen bestand das größte Risiko für eine Störung der Technologie nämlich in dem Erdbebengebiet. Bei den Spielen 2008 in Peking waren einige Dummy-Websites für den Kauf von gefälschten Geldscheinen eingerichtet worden. Doch erst seit dem Angriff auf die Eröffnungsfeier der Olympischen Spiele 2012 in London steht die Cybersicherheit ganz oben auf der Agenda der Organisatoren. **So hat sich die Zahl der Cyberangriffe innerhalb von zehn Jahren um das 20-fache** erhöht, von 212 Millionen bei den Spielen in London 2012 auf 4,4 Milliarden in Tokio 2021.

„Innerhalb von 10 Jahren hat sich die Zahl der Cyberangriffe so um das 20-fache erhöht, von 212 Millionen bei den Spielen in London 2012 auf 4,4 Milliarden in Tokio 2021."

London im Jahr 2012 ist das Ereignis, das den Beginn des cyberkriminellen Fokus auf die Olympischen Spiele markiert. Damals wurden bereits am Tag der Eröffnungsfeier mehr als 212 Millionen Cyberangriffe verzeichnet, die durch zahlreiche Offensiven wie Distributed Denial of Service (DDoS) auf die Strominfrastruktur.

Im Jahr 2014 dann, bei den Olympischen Winterspielen in **Sotschi,** gab es keinen größeren Cybersicherheitsvorfall, der in Erinnerung geblieben wäre. Geschlossene Kommunikation des russischen Staates, Desinteresse der Cyberkriminellen oder Angst vor Vergeltungsmaßnahmen? Die Frage bleibt offen ... Ein kleiner Hinweis auf die Antwort ist die Erklärung des FSB (Föderaler Sicherheitsdienst), der vorhatte, *„dafür zu sorgen, dass keine Kommunikation von Teilnehmern oder Zuschauern der Überwachung entgeht"*, indem er sich auf ein für diesen Anlass besonders verstärktes System zum Abfangen von Kommunikation stützte. Das US-Büro für diplomatische Sicherheit forderte seine Bürger auf, bei den Olympischen Spielen äußerste Vorsicht walten zu lassen. Eine Sensibilisierung der Athleten und US-Bürger für die Nichtweitergabe vertraulicher Daten, die so weit ging, dass man ihnen riet, so oft wie möglich den Akku aus dem Mobiltelefon zu nehmen.

Bei den Olympischen Spielen 2016 in **Rio** überschlugen sich die Zahlen mit einer halben Milliarde erfasster Cyberangriffe. Das sind 400 Angriffe pro Sekunde. So wurden Monate vor der Eröffnungsfeier in kurzen Abständen groß angelegte DDoS-Angriffe auf die Websites der Partnerorganisationen der Olympischen Spiele durchgeführt. Die Angriffe durch das LizardStresser-Botnet (das bereits durch die Sperrung der Online-Spieleplattformen PSN und Xbox Live in die Medien gelangt war) wurden dann während der Olympischen Spiele intensiviert, einschließlich einer DDoS-Kampagne mit über 500 Gbit/s.

Im Jahr 2018 intensiviert sich das Phänomen vor den Augen der Öffentlichkeit; denn es ist die Eröffnungsfeier der Spiele in **PyeongChang**, die davon betroffen ist. Einige Zuschauer konnten ihre Tickets nicht ausdrucken, um ins Stadion zu gelangen, es gab Probleme mit dem WLAN auf dem Gelände, die Zeremonie wurde nicht auf den Bildschirmen im Stadion übertragen, die RFID-Sensoren an den Zugangstüren funktionierten nicht, die offizielle Olympia-App funktionierte nicht (d. h. Zugang zum Ticketverkauf, Zeitpläne, Hotelinformationen, Zugangskarten usw.). Die Folgen waren schnell spürbar. Die Malware Olympic Destroyer richtet verheerende Schäden an, live vor Tausenden von Zuschauern und Journalisten. Es erforderte 12 Stunden harter Arbeit der Cybersicherheitsteams, um die IT-Infrastruktur der Olympischen Spiele aus den Backups zu rekonstruieren. Dieser ungewöhnliche Angriff wurde sofort zu einer internationalen Angelegenheit. Sie wurde Russland zugeschrieben und soll als Vergeltung für die Verbannung seiner Flagge bei dieser Ausgabe nach den Dopingfällen in Sotschi durchgeführt worden sein.

Im Jahr 2021 finden die Olympischen Spiele in **Tokio**, die wegen einer weltweiten Pandemie um ein Jahr verschoben wurden, unter Ausschluss der Öffentlichkeit statt. Trotzdem war auch diese Ausgabe nicht frei von Angriffen, da 4,4 Milliarden Cyberangriffe

auf die Organisation gestartet wurden. Laut der Nippon Telegraph and Telephone Corporation (NTT) wurden verschiedene Angriffsvektoren wie Phishing-E-Mails und gefälschte Websites, die die offiziellen Websites der Spiele nachahmten, eingesetzt. Ein hochrangiger japanischer Beamter gab an, dass die Olympischen Spiele Opfer eines Cyberangriffs waren, der ein Leck in den personenbezogenen Daten der Inhaber von Eintrittskarten für die Veranstaltung sowie der freiwilligen Helfer der Veranstaltung (Name, Adresse, Bankkontonummer) zur Folge hatte. Diese Daten wurden online offengelegt.

Im Jahr 2022 schließlich, während der Winterspiele in **Peking**, war es die offizielle Anti-Covid-19-App mit dem Titel My2022, die aus Angst vor Cyberspionage für Kontroversen sorgte. Eine Reverse-Engineering-Studie der Anwendung zeigte später, dass die Gespräche der Athleten auf chinesischen Servern gesammelt, analysiert und gespeichert wurden. Um dem entgegenzuwirken, gaben die Behörden vieler Länder ihren Delegationen daraufhin Anweisungen, wie z. B. die Empfehlung, ein Wegwerf-Handy mitzunehmen.

WIE WIRD DIE SICHERHEIT DER OLYMPISCHEN SPIELE IN PARIS 2024 VORBEREITET?

Das Organisationskomitee der Olympischen Spiele (OCOG) bereitet sich auf Cyberangriffe vor, da es aus den Erfahrungen der vergangenen Olympischen Spiele gelernt hat. **Tony Estanguet**, der Vorsitzende des Pariser OCOG 2024, zeigt sich klar und sagt im April 2021 gegenüber AFP: *„Wir zweifeln nicht daran, dass wir ständig angegriffen werden. An möglichen Zugängen für Mitarbeiter, über die Software, das Ökosystem darf es keinerlei Schlupflöcher geben."* Im Innenministerium betont **Ziad Khoury,** Präfekt und nationaler Sicherheitskoordinator für die Olympischen und Paralympischen Spiele 2024 (CNSJ), ebenfalls die Notwendigkeit der Cybersicherheit bei Großveranstaltungen und erklärte bei einem Treffen des Cercle des Assises de la Cyber im September 2021, dass *„jede Ausgabe der Olympischen Spiele neu ist, in dem Sinne, dass sie nicht mit den vorherigen verglichen werden können: Das Umfeld ändert sich, die Bedrohungen entwickeln sich weiter, sie werden immer vielfältiger und die Angriffe werden zahlreicher. Man kann aus früheren Erfahrungen lernen, muss sich aber vor allem auf das Unbekannte vorbereiten, da ein Teil der Bedrohungen für 2024 noch nicht bekannt ist."* Hinzu kommen die geopolitischen Konflikte in der Ukraine und die Empfehlung des Internationalen Olympischen Komitees (IOC) im Februar, Russland und Weißrussland von Sportwettkämpfen zu verbannen. Nicolas Caproni gesteht, dass *„Ransomware-Angriffe eine der Bedrohungen für die Olympischen Spiele sind. Sie wären jedoch nur ein Deckmantel für Sabotageakte mit dem Ziel, die Veranstaltung zu stören und das Image des Landes und der Olympischen Spiele zu beschädigen. Wenn Russland von der Veranstaltung 2024 ausgeschlossen bleibt, könnten wir Vergeltungsmaßnahmen befürchten."*

„Wir zweifeln nicht daran, dass wir ständig angegriffen werden. An möglichen Zugängen für Mitarbeiter, über die Software, das Ökosystem darf es keinerlei Schlupflöcher geben.

Tony Estanguet, Präsident des Pariser OCOG 2024

Um den immer zahlreicheren, komplexeren und innovativeren Cyberangriffen zu begegnen, organisieren sich die französischen Behörden. So unterzeichnete die ANSSI ein Kooperationsabkommen mit seinem japanischen Pendant, dem NISC (*National center of Incident readiness and Strategy for Cybersecurity*). Dies ist eine Gelegenheit, den Austausch und die Weitergabe von Erfahrungen rund um die Cybersicherheit bei großen Sportveranstaltungen wie der Rugby-Weltmeisterschaft und den Olympischen Spielen zu verstärken. Parallel dazu verstärkt das ANSSI seine Kommunikation, **um möglichst viele Menschen für digitale Hygiene zu sensibilisieren.** Es gibt zahlreiche Materialien wie den Reiseberatungspass, die 12 Regeln des gesunden Menschenverstands, die man im digitalen Alltag anwenden sollte, oder den Leitfaden für gute Computerpraxis. Das Innenministerium seinerseits behauptet, den sogenannten „intelligenten" Videoschutz entwickeln zu wollen. Diese Kameras wären in der Lage, verdächtiges Verhalten, Bewegungen von Menschenmengen dank künstlicher Intelligenz in Echtzeit zu erkennen. Der Einsatz von Gesichtserkennung im öffentlichen Raum, der mangels angemessener Gesetze zur Gewährleistung des Datenschutzes eingestellt worden war, rückt wieder in den Vordergrund. Laut Vincent Riou, der die Arbeit der Alliance pour la Confiance Numérique (ACN) zitiert, *„wäre es angebracht, unsere nationalen Technologien zu fördern, da die Olympischen Spiele ein wunderbares Schaufenster für unsere französische Cyberindustrie und generell unsere Industrie für digitale Sicherheit darstellen"*.

Auf der organisatorischen Seite beläuft sich **das Budget für die Olympischen Spiele in Paris zum Thema Cybersicherheit auf über 17 Millionen Euro.** Es umfasst ein Präventions- und Abwehrprogramm mit lebensgroßen Simulationen, sicherem Anwendungscode, Bemühungen um die Abdichtung der Netzwerk- und Serverschichten bei der Gestaltung von Infrastrukturen, Sicherheitsprüfungen oder auch die Einrichtung von SOCs. Außerdem wird ein Sensibilisierungsprogramm mit Schulungen für Mitarbeiter, Sponsoren, Subunternehmer, Athleten und alle anderen Beteiligten durchgeführt, das von einem strengen Pflichtenheft begleitet wird, das der gesamten Kette der Subunternehmer auferlegt wird. **Anne Le Hénanff**, Inhaberin des Lehrstuhls für Cybersicherheit bei Großveranstaltungen an der Universität Bretagne Sud, betonte ihrerseits die Rolle der lokalen Behörden, die Delegationen auf ihrem Gebiet empfangen werden, und wie wichtig es sei, sie in dieses Cyber-Thema einzubinden. Anlässlich eines Symposiums im Februar zum Thema *„Der Erfolg der Olympischen Spiele Paris 2024, eine entscheidende Herausforderung für die Cybersicherheit"* sensibilisiert sie dafür, dass: *„Die Behörden sind zwar zu Recht auf Fragen der physischen Sicherheit und der Steuerung von Personenströmen fokussiert, aber sie sind nicht für die Cybersicherheitsproblematik sensibilisiert. Ihr Kompetenzaufbau in diesem Bereich ist eine Grundvoraussetzung für den Erfolg der Olympischen Spiele."*

In Anlehnung an frühere Austragungen ist die Cyberbedrohung für die Olympischen und Paralympischen Spiele in Paris 2024 die staatliche Störung. **Angesichts der Gefahr von Terroranschlägen oder anderen Problemen der inneren Sicherheit sollte die Cybersicherheit nicht als Silo betrachtet werden, sondern als Teil des Sicherheitsprogramms der Veranstaltung**. Für Vincent Riou ist es undenkbar, die physische Sicherheit von der Cybersicherheit zu entkoppeln und den zunehmend hybriden Charakter von Cyberbedrohungen zu berücksichtigen. *„Einige Angreifer könnten versucht sein, bestimmte Systeme anzugreifen, um ohne Zugangsberechtigung in die Arenen zu gelangen, oder sie könnten bewirken, dass die Zuschauer die Arenen verlassen und sich außerhalb der geschützten Arenen sammeln, was Terroranschläge erleichtern würde. Cyberangriffe werden so zu Erleichterungen für Angriffe mit großer Wirkung. Die Cybersicherheit ist ein integraler und nicht ein separater Bestandteil des gesamten Sicherheitssystems der Spiele."*

In dem kürzlich erschienenen Bericht der Senatoren Meurant und Cardon über die Cybersicherheit wird das klare Ziel formuliert, *„die französische Industrie als Weltmarktführer im Bereich der Cybersicherheit und der Sicherheit des Internets der Dinge zu positionieren"*. Die Olympischen Spiele in Paris 2024 wären dann eine großartige Gelegenheit dazu. Französische Behörden, OCOG, Partnerunternehmen und Sponsoren, Cybersicherheitsunternehmen ... alle vereint, um dieses Ereignis sicher zu gestalten, um den Feierlichkeiten Raum zu geben. Nach der (missglückten) Episode mit dem Champions-League-Finale bietet sich die Rugby-Weltmeisterschaft 2023 in Frankreich als Aufholjagd an.