BEZPIECZEŃSTWO • 2019 nr 2 TEORIA I PRAKTYKA
e-ISSN 2451-0718
ISSN 1899-6264
DOI: 10.34697/2451-0718-btip-2019-2-006

Maciej Saskowski
doktorant, Krakowska Akademia im. Andrzeja Frycza-Modrzewskiego
ORCID: 0000-0003-1611-7062

Wielkie imprezy sportowe a nowe technologie: trendy w cyberzagrożeniach

Wprowadzenie

Wyobraźmy sobie taki scenariusz: zimowe igrzyska olimpijskie w 2030 r., łyżwiarski program dowolny mężczyzn został przerwany w połowie zawodów. Kilka państw zgłasza protest, twierdząc, że nowy system punktacji elektronicznej, wykorzystujący sztuczną inteligencję do oceny wysokości skoków łyżwiarzy i liczby obrotów piruetów, błędnie ocenia zawodników. Wezwana jest firma zajmująca się cyberbezpieczeństwem, która wkrótce odkrywa najgorszy koszmar organizatorów: system został zhakowany, a wyniki – wypaczone. Czy rywalizacja zostanie wznowiona w późniejszym terminie lub ponownie oceniona przez sędziów wykorzystujących nagrania telewizyjne?

Z zakwestionowaniem wiarygodności wyników najważniejszych imprez sportowych mieliśmy do czynienia jeszcze przed erą digitalizacji. W finale gimnastycznym igrzysk olimpijskich w Sydney w 2000 r. wysokość sklepienia konia została niewłaściwie ustawiona, co spowodowało, że zawodniczki, wykonujące obroty nad przyrządem, popełniały błędy. Dopiero jeden z australijskich sportowców zauważył nieprawidłowe ustawienie. Poszkodowane zawodniczki mogły powtórzyć swój skok pod koniec zawodów; niestety, kilka kluczowych gimnastyczek, w tym faworytka Swietłana Chorkina, zdekoncentrowane, popełniły dodatkowe błędy, zaprzepaszczając szanse na olimpijki tytuł[1].

[1] E. Pells, *Gymnastics: Olympic Vault Set Too Low*, ABC News, http://abcnews.go.com/Sports/story?id=100494&page=1 [dostęp: 27.03.2019].

Jednak digitalizacja najważniejszych wydarzeń sportowych stwarza oprócz ryzyka również nowe kierunki rozwoju. Z jednej strony rośnie zagrożenie cyfrowymi oszustwami, wynikające z przenikania nowych technologii do treningu sportowców, odbioru wydarzeń sportowych przez kibiców czy wreszcie procederów, które doprowadzają m.in. do manipulacji wynikami. Wszystkie przytoczone przykłady zapewniają uatrakcyjnienie sposobu uprawiania sportu i doświadczania go, ale umożliwiają również atak na jego uczciwość. Sport już dziś jest integralną częścią systemu informatycznego, co umożliwia cyberprzestępcom zakłócanie przebiegu imprez sportowych z zacisza własnego domu.

Z drugiej strony pokusa manipulowania ważnymi wydarzeniami sportowymi może się tylko nasilać. Takie imprezy są coraz bardziej popularne i coraz bardziej zyskowne[2], a ich intratność wiąże się ze wzrostem inwestycji pieniężnych w sportowy przemysł. Przybywa sposobów, jakimi społeczeństwo, wykorzystując nowe technologie, może angażować się w sport. Szczególnym zagrożeniem jest hazard sportowy, wraz ze wzrostem popularności „zakładów bukmacherskich na żywo"[3], w przypadku których hazardziści mogą odnosić korzyści już w trakcie trwania zawodów, bez konieczności obstawiania wyniku końcowego.

Rozważmy przykład tenisa. W spotkaniach, w których jest obecna technologia Hawk-Eye (znana także jako *challenge*, „sokole oko", „jastrzębie oko" – system, który ocenia, czy piłka znajduje się na korcie tenisowym, czy poza nim), pełni okna rolę ostatecznego arbitra dla każdego gracza, który poprosi o tzw. „challange". Wyobraźmy sobie, że ten system zostałby zhakowany tak, że co piąte użycie Hawk-Eye faworyzowałoby konkretnego gracza. Kto wykryłby różnicę? Czy sprytny hazardzista byłby w stanie przewidzieć ostateczny wynik meczu? Jaką mamy pewność, czy ten rodzaj korupcji już nie istnieje? (każdy widz tenisowy z pewnością obserwował wywoływane „challange", które wyglądały gołym okiem, jakby miały być autowe, a Hawk-Eye uznawał je za prawidłowe).

Celem niniejszego artykułu jest wskazanie trendów w cyberzagrożeniach[4] podczas wielkich imprez sportowych, jakimi są igrzyska olimpijskie. Jak zmieni się sport? Jakie nowe technologie wpłyną na zmiany sposobu postrzegania roli dużych wydarzeń sportowych?

W celu oceny powagi wpływu cyberataków na ważne wydarzenia sportowe artykuł rozpoczyna się określeniem zakresu ryzyka – analizą zagrożeń i ich konsekwencji. Następnie autor dokonuje przeglądu przypadków hakowania dużych wydarzeń sportowych, kategoryzując je według przyjętych ram. Wreszcie, koncentrując się na igrzyskach olimpijskich, a zwłaszcza na czterech dyscyplinach – gimnastyce, wioślarstwie, pływaniu i lekkoatletyce –omawia różne potencjalne przyszłe zagrożenia. Artykuł kończy się wnioskami autora oraz przedstawieniem propozycji metod walki z cyberzagrożeniami w sporcie.

---

2 *Coraz większe zyski MKOl, ale chętnych do organizacji igrzysk ubywa*, Interia, 30.01.2018, https://sport.interia.pl/raporty/raport-pjongczang-2018/aktualnosci/news-coraz-wieksze-zyski-mkol-ale-chetnych-do-organizacji-igrzysk,nId,2515781 [dostęp: 27.03.2019].

3 S. Stinson, *If Leagues Decide Gambling Can Help Grow Their Games, Trump Could Help Deliver*, National Post, 4.03.2017, https://nationalpost.com/sports/if-leagues-decide-gambling-can-help-grow-their-games-trump-could-help-deliver [dostęp: 27.03.2019].

4 Niniejszy artykuł nie koncentruje się na cyberbezpieczeństwie e-sportu.

Ramowe zasady pomiaru ryzyka cyberzagrożeń w sporcie

Wydaje się oczywiste, że nie wszystkie cyberzagrożenia są sobie równe. Jednak jeśli chodzi o ważne wydarzenia sportowe, nie podjęto spójnych działań mających na celu skategoryzowanie zagrożeń związanych z tego typu wydarzeniami i/lub umożliwienie odpowiednim służbom nadanie priorytetu różnym rodzajom cyberniebezpieczeństw.

W niniejszym artykule autor posługuje się techniką analizy rodzajów i skutków możliwych błędów FMEA (ang. *failure mode and effects analysis*). Metoda ta ma na celu zapobieganie skutkom wad, które mogą wystąpić w fazie projektowania oraz w fazie wytwarzania. FMEA ma trzy wymiary: 1. stopień zakłócenia lub jak poważny może być negatywny wynik; 2. występowanie lub jak prawdopodobny bądź częsty może być wynik negatywny; oraz 3. wykrywalność lub prawdopodobieństwo, że negatywny wynik nie zostanie wykryty[5]. Ramy te nie są zwykle używane do oceny zagrożeń związanych z cyberbezpieczeństwem, ale stanowią użyteczną metodę ważenia różnych incydentów cybernetycznych. Poniżej przedstawiono ramowe zasady dla pomiaru ryzyka w najważniejszych wydarzeniach sportowych.

1. Stopień zakłócenia. Ataki hakerów możemy kategoryzować na podstawie stopnia, w jakim dane cyberzagrożenie może zakłócić prawidłowy przebieg wydarzenia sportowego. Najpoważniejsze byłoby fizyczne uszkodzenie sportowców lub widzów; w takim przypadku impreza sportowa zostanie prawdopodobnie odwołana w wyniku zaistniałych poważnych obrażeń. Podobnie zniszczenia powstałe w miejscu rozgrywek sportowych mogłyby skutkować odwołaniem imprezy. Ataki na integralność wydarzenia sportowego byłyby równie poważne; ingerencja w wyniki sportowców może spowodować utratę poczucia zaufania co do uczciwości sportu. Wszystkie trzy wymienione kategorie miałyby oczywiście skutki finansowe; jednak takie szkody wiązałaby się z czysto finansowymi efektami, które nie wpływałyby na przebieg rywalizacji i infrastrukturę sportową. Ostatnia kategoria to utrata reputacji: cyberataki mogą zasiewać wątpliwości co do wiarygodności i transparentności organizacji sportowych i ich zdolności do radzenia sobie w sytuacjach kryzysowych.

2. Prawdopodobieństwo wystąpienia szkodliwego zdarzenia. Ponownie różni się to znacznie w zależności od specyfiki, ale mniej więcej pokrywa się z liczbą kluczowych obszarów, którymi cyberprzestępca może manipulować, aby wpłynąć na wydarzenie sportowe. Im mniej takich obszarów wystąpienia cyberataku, tym mniejsze zagrożenie. W najmniejszym stopniu prawdopodobne są ataki terrorystyczne mające na celu wyrządzenie szkody fizycznej, ponieważ ataki fizyczne przy użyciu narzędzi cybernetycznych są stosunkowo trudne do przeprowadzenia. Nieco bardziej prawdopodobne jest zakłócenie wyniku rywalizacji sportowej, zwłaszcza że można na to wpłynąć na wiele różnych sposobów, jak choćby manipulując ocenami sędziów. Jeszcze bardziej prawdopodobne są straty finansowe, ponieważ w trakcie ważnego wydarzenia sportowego w użyciu jest wiele systemów płatniczych, w których cyberprzestępcy mogą dokonywać manipulacji. Wreszcie zagrożenia dla reputacji, ponieważ dotykają każdego aspektu ważnego wydarzenia sportowego; każdy negatywny efekt cyberataku może zaszkodzić reputacji imprezy.

---

[5] S. Wawak, B. Turek, *Analiza FMEA*, Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Analiza_FMEA, [dostęp: 27.03.2019].

W sportach olimpijskich, o których mowa w niniejszym artykule, nasilenie i występowanie są ściśle powiązane. Im bardziej prawdopodobne, że cyberzagrożenie spowoduje znaczne szkody, tym mniejsze prawdopodobieństwo jego wystąpienia. I odwrotnie: bardziej prawdopodobne jest wystąpienie cyberzagrożeń, które mogą powodować znaczne szkody. Chociaż mogą wystąpić zagrożenia, które są zarówno bardzo prawdopodobne, jak i mogą spowodować znaczną szkodę. (Oczywiście istnieją też zagrożenia, które prawdopodobnie nie powodują szkód i które prawdopodobnie nie wystąpią, ale nie są one przedmiotem badań autora).

Jedną z głównych przyczyn współzależności stopnia zakłócenia z prawdopodobieństwem jego wystąpienia jest to, że wydarzenia sportowe od dawna są uznane za imprezy podwyższonego ryzyka i istnieją już dla nich odpowiednie protokoły bezpieczeństwa, które próbują zapobiegać zagrożeniom. Na długo przed pojawieniem się technologii cyfrowych uznano, że wydarzenia sportowe to idealny cel dla przestępców: duże tłumy, ogromne stadiony i hale nie są łatwe do ochrony. W rezultacie obiekty sportowe rozwinęły infrastrukturę – m.in. systemy do prześwietlania o zaawansowanej technologii wykorzystywane przy kontroli widzów czy bramki przy wejściach na obiekty – zapobiegającą ewentualnym katastrofalnym skutkom niebezpiecznych sytuacji. Ponieważ w świecie analogowym w grę wchodzi tych samych pięć wymienionych kategorii szkód, od szkód fizycznych do reputacyjnych – istnieje już infrastruktura, która ma im zapobiec. Dzięki temu zminimalizowano prawdopodobieństwo wystąpienia groźnych incydentów.

3. Poziom wykrywalności. Niejako dodatkową, trzecią kategorią w analizie rodzajów błędów oraz ich skutków FMEA jest wykrywalność. Niewykryty cyberatak może powodować dalsze szkody, powiększając te już powstałe. Rzadziej wykrywalne cyberprzestępstwa mogą powtarzać się (np. przez wielokrotnie wykorzystywane luki systemowe), prowadząc do wielu niepożądanych zniszczeń.

Nie każde niewykrywalne zdarzenie będzie niepokojące; mogą wystąpić małe niewykryte zakłócenia, które powodują ograniczone szkody. Brak wykrywalności może wpływać na to, jak postrzegamy szkodliwość cyberataku. Cyberprzestępstwo, które ma niską wykrywalność, może wydawać się mniej poważne w skutkach niż jest w rzeczywistości.

Przedstawione ramy stanowią przydatny sposób na ocenę, które spośród wielu cyberzagrożeń podczas trwania najważniejszych imprez sportowych powinny mieć priorytet. Ogólnie rzecz ujmując, cyberataki z najmniej tolerowanym poziomem ryzyka powinny być traktowane priorytetowo, ponieważ ich skutki mogą być większe. Co więcej, biorąc pod uwagę, że takie ataki są rzadsze, łatwiej będzie je zwalczać niż próbować zniwelować wiele różnych, rozproszonych zagrożeń.

W dalszej części artykułu, przyjmując dotychczasowe założenia, ocenie poddane zzostaną cyberzagrożenia podczas wielkich imprez sportowych. W pierwszej kolejności te znane z historii olimpizmu, a następnie możliwe przyszłe zagrożenia, wynikające z rozwoju technologii.

Współczesne cyberzagrożenia w sporcie

Wśród cyberzagrożeń występujących podczas wielkich imprez sportowych można wyróżnić cztery kategorie:

- infiltracja sportowych stron internetowych i systemów informatycznych;
- oszustwa związane z dystrybucją biletów;
- hakowanie i udostępnianie wrażliwych danych sportowca;
- ryzyko zhakowania kibiców uczestniczących w imprezie sportowej[6].

Po pierwsze: podobnie jak w przypadku każdego innego systemu podłączonego do Internetu, hakerzy mogą próbować manipulować treścią lub zakłócać funkcjonowanie witryn sportowych i systemów poczty elektronicznej. Na przykład grupa hakerów Anonymous włamała się w 2012 r. na stronę internetową Formuły 1, protestując przeciwko organizacji wyścigu Grand Prix w Królestwie Bahrajnu[7]. W 2014 r. sympatycy ISIS zaatakowali i zlikwidowali stronę internetową klubu rugby English League[8]. Celem cyberprzestępców były również organizacje, które wspierają ważne wydarzenia sportowe. Podczas Mistrzostw Świata w 2014 r. brazylijscy urzędnicy stali się ofiarami ataków phishingowych, przeprowadzonych przez tzw. „haktywistów", którzy z powodzeniem infiltrowali konta e-mailowe wielu urzędników Ministerstwa Spraw Zagranicznych pomagających w organizacji mundialu[9]. Jednym z powtarzających się sposobów cyberataków jest wykorzystanie DDoS (ang. *distributed denial of service*, rozproszona odmowa usługi) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów, np. brazylijskie Mistrzostwa Świata w Piłce Nożnej były wielokrotnie atakowane z wykorzystaniem DDoS. Hakerom udało się zlikwidować m.in. stronę internetową brazylijskiego Ministerstwa Sportu[10]. Również podczas Igrzysk Olimpijskich w Rio 2016 organizatorzy walczyli o utrzymanie oficjalnej strony zawodów, która poddawana była licznym atakom DDoS[11].

---

[6] Niewiele jest tekstów w języku polskim łączących cyberbezpieczeństwo i ważne wydarzenia sportowe. Nieliczne pochodzą ze stron internetowych związanych z cyberbezpieczeństwem, np.: K. Kochetkova, *Trendy w cyberzagrożeniach podczas Igrzysk Olimpijskich*, Kaspersky Lab, 19.07.2016, https://plblog.kaspersky.com/olympic-games-2016-threats-guide/5152; *Zobacz, jakie ataki szykują hakerzy na igrzyska olimpijskie*, eGospodarka.pl, 18.02.2018, http://www.egospodarka.pl/146729,Zobacz-jakie-ataki-szykuja-hakerzy-na-igrzyska-olimpijskie,1,12,1.html; *Cyberbezpieczeństwo na międzynarodowych imprezach sportowych, takich jak Mistrzostwa Świata w Piłce Nożnej 2018*, itd24.pl, 18.07.2018, https://itd24.pl/quick-heal-seqrite/cyberbezpieczenstwo-na-miedzynarodowych-imprezach-sportowych-takich-jak-mistrzostwa-swiata-w-pilce-noznej-2018; *Cyberbezpieczeństwo na arenach sportowych*, 4safe.pl, 15.09.2016, http://www.4safe.pl/wiadomosci/10/cyberbezpieczenstwo_na_arenach_sportowych [dostęp do wszystkich wymienionych artykułów: 27.03.2019]. Artykuły koncentrują się na cyberatakach na infrastrukturę komputerową podczas ważnych wydarzeń sportowych, a nie – w jaki sposób cyberzagrożenia mogą wpłynąć na przebieg imprez sportowych.

[7] A. Nowak, *Anonymous zaatakowali strony Formuły 1*, „Bezpieczeństwo. Dziennik Internautów", 23.04.2012, http://di.com.pl/anonymous-zaatakowali-strony-formuly-1-44876 [dostęp: 27.03.2019].

[8] J. Hampshire, *Professional Sports Teams Are Risking a Cybersecurity Own Goal*, Infosecurity Group, 11.08.2015, https://www.infosecurity-magazine.com/opinions/professional-sports-teams [dostęp: 27.03.2019].

[9] F. Guerrini, *Brazil's World Cup of Cyber Attacks: From Street Fighting to Online Protest*, Forbes, 17.06.2014, https://www.forbes.com/sites/federicoguerrini/2014/06/17/brazils-world-cup-of-cyber-attacks-from-street-fighting-to-online-protest/#49874ca251a8 [dostęp: 27.03.2019].

[10] *Ibidem*.

[11] D. Bisson, *How A Massive 540 Gb/Sec DDoS Attack Failed to Spoil the Rio Olympics*, Tripwire, 5.09.2016, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics [dostęp: 27.03.2019].

Mimo ogromnej ilości ataków hakerskich podczas wielkich imprez sportowych – podczas igrzysk w Pekinie doliczano się 11–12 mln codziennych alarmów[12] – tylko kilka uznano za bezpośrednie zagrożenie. Organizatorzy Igrzysk Olimpijskich w Londynie zgłosili Głównemu Oficerowi Informacyjnemu Igrzysk sześć poważnych incydentów zagrażających bezpieczeństwu. Pięć z tych zdarzeń dotyczyło ataków DDoS lub podobnych ataków (np. zainfekowana wirusami agencja reklamowa powiązana z igrzyskami wysyłała tyle spamu, że adres IP używany przez inne agencje prasowe został zablokowany)[13].

Po drugie: cyberataki na serwisy online związane ze sprzedażą biletów, rezerwacjami, miejscami na trybunach, hotelami, usługami transportowymi oraz zamawianiem jedzenia. Pogoń kibiców za biletami na najważniejsze imprezy sportowe przyciąga uwagę spamerów, którzy dostrzegają dobrą okazję zarobienia pieniędzy kosztem łatwowiernych osób. Niektórzy fani, zaślepieni blaskiem sportowej rywalizacji, zrobią wiele, by zdobyć upragnione wejściówki. A oszuści, wykorzystując naiwność sportowych fanów, wysyłają do nich wiadomości, w których próbują przekonać ofiary, że to właśnie ich adres e-mail został wylosowany z długiej listy chętnych. Aby odebrać nagrodę, należy odpowiedzieć na e-mail, podając swoje dane osobowe i informacje o karcie kredytowej lub kliknąć zainfekowaną stronę internetową. Często sprawcy cyberprzestępstw stosują techniki oszustwa powszechnie stosowane gdzie indziej, takie jak rzekome zwycięstwo na loteriach. Podczas igrzysk olimpijskich w Londynie w 2012 r. oszuści wysyłali wiadomości e-mail informujące odbiorców, że wygrali loterię związaną z olimpiadą; ci, którzy uwierzyli w oszustwo, zostali poproszeni o uiszczenie „opłat manipulacyjnych”[14]. Równie ryzykowna jest odsprzedaż biletów. W 2015 r. hakerzy zamierzali przejąć sprzedaż biletów na Mistrzostwa Świata w Rugby, aby wymusić odsprzedaż na rynkach wtórnych i podnieść ceny biletów[15].

Po trzecie: ataki na pracowników i uczestników zawodów (phishing, ataki hakerskie, zdalne monitorowanie lub manipulowanie danymi, szantaż). Wrażliwe dane sportowców są cenne dla każdej federacji sportowej, przez co groźba kradzieży takich danych jest niezwykle wysoka. W 2015 r. hakerzy uzyskali dostęp do danych dotyczących wydajności czołowego kolarza Chrisa Froome’a, próbując go zdyskredytować[16]. Hakerzy wykradli również poufne dane Światowej Agencji Antydopingowej (WADA) i opublikowali listy, którym olimpijczykom z Rio przyznano zwolnienie z obowiązku przyjmowania leków normalnie niedozwolonych z powodu właściwości

[12] *Securing the 2012 Olympics*, Infosecurity Group, 19.11.2009, https://www.infosecurity-magazine.com/magazine-features/securing-the-2012-olympics [dostęp: 27.03.2019].

[13] G. Burton, *How the London Olympics Dealt With Six Major Cyber Attacks*, Computing, 6.03.2013, https://www.computing.co.uk/ctg/news/2252841/howthe-london-olympics-dealt-with-six-major-cyber-attacks#comment_form [dostęp: 23.03.2019].

[14] *Więcej złośliwego oprogramowania podczas Olimpiady 2012*, WebSecurity, 6.08.2012, http://websecurity.pl/tag/olimpiada [dostęp: 23.03.2019].

[15] B. Rumsby, *Rugby World Cup 2015 Tickets: Cyber Criminals Plotting to Hijack Launch*, The Telegraph, 11.09.2014, http://www.telegraph.co.uk/sport/rugbyunion/rugby-world-cup/11088098/Rugby-World-Cup-2015-tickets-Cyber-criminals-plotting-to-hijack-launch.html [dostęp: 23.03.2019].

[16] *Lider Tour de France zaatakowany przez hakerów!*, Fakt24, 15.07.2015, https://www.fakt.pl/sport/inne-sporty/hakerzy-przypuscili-atak-na-lider-tdf-chrisa-frooma/xexweqr [dostęp: 23.04.2019].

zwiększających wydajność organizmu[17]. Z wykradzionych tajnych dokumentów WADA wynikało, że wielu sportowców z pierwszych stron gazet miało ciche przyzwolenie na zażywanie dopingu. Hakerzy wykradli między innymi dane gimnastyczki Simon Biles oraz tenisistek Venus i Sereny Williams. Do kradzieży informacji przyznała się grupa Fancy Bears[18].

Po czwarte: fani reprezentują grupę narażoną na cyberzagrożenia podczas dużych imprez sportowych z powodu zwiększonego wykorzystania urządzeń elektronicznych, niskiego poziomu zabezpieczeń i zwiększonych pokładów kreatywności cyberprzestępców[19]. Podczas Zimowych Igrzysk Olimpijskich w Soczi „NBC News" w swoich doniesieniach, próbowało zademonstrować łatwość, z jaką osobiste urządzenia fanów mogły być zhakowane[20]. Chociaż raport powszechnie uznano za niewykazujący luk w zabezpieczeniach igrzysk olimpijskich[21], pokazał jednak, że kibice są szczególnie narażeni na cyberprzestępstwa.

Przytoczone przykłady cyberzagrożeń charakteryzują się wspólnym motywem: uzyskanie dostępu lub kontrola nad systemami komputerowymi używanymi do przechowywania danych sportowych lub danych kibiców. Głównymi celami cyberataków są reputacja lub finanse; hakerzy albo próbują wpłynąć na wizerunek sportu, albo próbują szybko zarobić. Jedyny wyjątek: włamanie do bazy WADA i publikacja danych sportowców startujących podczas Igrzysk Olimpijskich w Rio, które było nie tylko nieetyczną próbą zburzenia reputacji imprezy sportowej, ale także podważało prawdziwość osiągniętych wyników sportowych.

Warto zauważyć, że do tej pory cyberprzestępstwa nie wpłynęły znacząco na sam przebieg wydarzenia sportowego, jednak obawa przed takim aktem nie jest całkowicie bezzasadna. Podczas Igrzysk Olimpijskich w Londynie w 2012 r. istniało wiarygodne zagrożenie, że sieć elektryczna zostanie zhakowana, odcinając zasilanie podczas ceremonii otwarcia. Na szczęście zagrożenie było fałszywym alarmem; mimo to takie incydenty uczulają organizatorów na przyszłość[22].

Przewidywalne trendy cyberzagrożeń

Chociaż pojawiły się powszechne obawy co do roli, jaką hacking może odgrywać w przebiegu wydarzeń sportowych, przytoczony przykład londyńskich igrzysk

---

17 *Rosyjscy hakerzy wykradli dane medyczne sportsmenek z Rio*, Wprost, 13.09.2016, https://www.wprost.pl/sport/10023047/Rosyjscy-hakerzy-wykradli-dane-medyczne-sportsmenek-z-Rio.html [dostęp: 23.03.2019].

18 *Ibidem*.

19 A. Brill, S. Petreska, *Are Cyber Criminals Competing at the Olympics?*, Freedom From Fear Magazine, 24.05.2016, http://insct.syr.edu/wp-content/%20uploads/2015/05/Brill_Olympics.pdf [dostęp: 23.03.2019].

20 *Hacked within Minutes: Sochi Visitors Face Internet Minefield*, NBC News, 4.02.2014, http://www.nbcnews.com/video/nightly-news/54273832#54273832 [dostęp: 23.03.2019].

21 J.A. Kaplan, *NBC News Takes Heat over Sochi Phone Hacking Report*, Fox News, 7.02.2014, http://www.foxnews.com/tech/2014/02/07/nbc-news-takesheat-over-sochi-phone-hacking-report.html [dostęp: 23.03.2019].

22 G. Corera, The 'Cyber-Attack' Threat to London's Opening Ceremony, BBC News, 8.07.2013, http://www.bbc.com/news/uk-23195283 [dostęp: 23.03.2019].

sugeruje, że obawy te w dużej mierze dotyczą systemów cyfrowych i podstawowego sprzętu komputerowego (w tym telefonów). Eksperci do spraw bezpieczeństwa cybernetycznego obawiali się, że podczas ataku systemy te mogą zostać zniszczone lub przejęte przez niebezpieczne podmioty. Z racji, że systemy te były w dużej mierze odseparowane od przebiegu samej rywalizacji sportowców, organizatorzy wraz za służbami odpowiedzialnymi za cyberbezpieczeństwo nie martwili się, w jaki sposób hakerzy mogą wpływać na integralność wyników lub jak mogą zakłócać działanie systemów na stadionach, powodując tym samym negatywny odbiór przez kibiców sportowych.

To się zmieni – i to szybko. Rozprzestrzenianie się Internetu rzeczy (również Internetu przedmiotów, ang. *Internet of Things* – IoT) – koncepcji, wedle której jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej inteligentnej KNX lub sieci komputerowej, zmienia oblicze cyberbezpieczeństwa sportu, dodając cyfrowe wymiary tam, gdzie ich wcześniej nie było. Technologie cyfrowe są włączane w każdy aspekt rywalizacji sportowej, od systemów punktacji po monitoring sportowców, od „inteligentnych" stadionów po infrastrukturę przeznaczoną dla kibiców. Wśród trendów można wymienić:

- zwiększoną kwantyfikację systemów pomiaru wyników, wymagającą szczegółowych systemów punktacji liczbowej;
- podglądy wideo obejmujące technologię mającą ułatwić podejmowanie decyzji przez sędziów;
- zwiększone zainteresowanie gromadzeniem danych na temat wyników i treningów sportowców;
- proliferacja technologii operacyjnych na terenie obiektów sportowych: np. ogrzewanie, wentylacja, klimatyzacja, windy, oświetlenie awaryjne, sygnalizacja świetlna;
- wzrost liczby urządzeń mobilnych umożliwiających śledzenie danych;
- immersyjność – proces zanurzania albo pochłaniania kibiców sportowych przez rzeczywistość elektroniczną, w tym rzeczywistość wirtualną, ale również kamery monitorujące i drony.

Technologizacja sportu będzie trwała, a nawet przyspieszy w ciągu najbliższych kilku lat. Należy zatem zadać pytanie, w jaki sposób ruch olimpijski może przygotować się na czekające go niebezpieczeństwa związane z cyfryzacją sportu.

Metodologia badań

Dostępne rozwiązania w zakresie prognozowania przyszłych cyberzagrożeń są niewystarczające i należy poszukiwać innych metod, umożliwiających precyzyjniejsze ich przedstawienie. Kolejna część artykułu prezentuje oryginalne rozwiązanie, wykorzystujące regresję, która na podstawie kształtowania się dotychczasowych cyberzagrożeń jest w stanie z dużym prawdopodobieństwem wyznaczyć przyszłe ich trendy.

Do tego celu autor wykorzystał metodę prognozowania, w tym konkretnym przypadku – prognozowania cyberzagrożeń, które odnosi się do przewidywania prawdopodobnych sytuacji kryzysowych związanych z cyberbezpieczeństwem na podstawie

zdarzeń już wcześniej poznanych i trendów panujących w czasie teraźniejszym. Wśród wykorzystanych metod znalazł się przegląd literatury oraz obserwacje blisko 10 głównych wydarzeń sportowych. Autor niniejszego artykułu pragnie podkreślić, że nie ma na celu przewidywania przyszłości, ale raczej zilustrowanie zakresu możliwości, które mogą się kiedyś rozwinąć.

Należy zwrócić uwagę, że rodzaje incydentów hakerskich opisanych w niniejszym artykule – oszustwa biletowe, manipulacja stronami internetowymi itp. – prawdopodobnie nie zmienią się, ale ponieważ zagrożenia te są już dobrze rozpoznane, poniższa analiza koncentruje się głównie na nowych trendach cyberzagrożeń.

Analiza cyberzagrożeń wielkich imprez sportowych

Integralność fizyczna

Najpoważniejsze potencjalne cyberataki podczas dużych imprez sportowych to takie, które mogą prowadzić do obrażeń ciała widzów, sportowców, działaczy sportowych lub innych uczestników. Takie ataki są niezwykle rzadkie i często polegają na atakowaniu infrastruktury – systemów bezpieczeństwa, transportu, urządzeń medycznych – zaprojektowanej w celu ochrony życia ludzkiego.

Chociaż można sobie wyobrazić, że urządzenia cyfrowe mogą być manipulowane w celu umożliwienia fizycznego uszkodzenia ciała sportowca – na przykład skaner ciała może zostać zhakowany, żeby umożliwić terrorystom posiadającym broń wejście na teren obiektu sportowego, lub dowolny pojazd mechaniczny może być kontrolowany zdalnie w celu zranienia sportowców lub widzów – takie incydenty są mało prawdopodobne, ponieważ wymagają skomplikowanych przygotowań. Mimo to, zwłaszcza gdyby taki atak był koordynowany w wielu lokalizacjach, skutki mogą być katastrofalne.

Bardziej prawdopodobna wydaje się sytuacja, kiedy widzowie lub sportowcy mogą ponieść szkody fizyczne w wyniku zdarzeń wywołujących panikę, spowodowaną niedozwolonym naruszeniem systemu komputerowego. Na przykład podłączona do sieci tablica cyfrowa na stadionie może zostać zhakowana, żeby powiadomić fanów o zagrożeniu terrorystycznym oraz informując ich, że powinni jak najszybciej opuścić obiekt sportowy. Nawet jeśli alarm będzie fałszywy, panika, która zostanie wywołana, mogłaby spowodować obrażenia fizyczne u widzów próbujących wydostać się ze stadionu.

Warto zauważyć, że wszystkie te incydenty – atak terrorystyczny, wypadki komunikacyjne lub panika w tłumie – mogą wystąpić nawet bez interwencji technologii cyfrowej. Hakowanie polega na ingerowaniu w tradycyjne systemy bezpieczeństwa (skanery bezpieczeństwa, pojazdy mechaniczne, wyjścia awaryjne), usuwając z nich czynnik fizyczny, którym nie można było tak łatwo zmanipulować w czasach analogowych.

Integralność obiektu sportowego

Druga kategoria ataków obejmuje te, które zakłócają integralność obiektu sportowego, ale nie powodują szkód fizycznych u sportowców lub widzów. W takich

przypadkach głównym poszkodowanym jest sama impreza sportowa, ponieważ wydarzenie nie będzie mogło się odbyć zgodnie z planem.

Przede wszystkim chodzi o ataki na infrastrukturę sportową, tak jak miało to miejsce w przypadku igrzysk w Londynie; utrata zasilania przez sieć elektryczną pozostaje poważnym problemem, aczkolwiek dobrze chronionym. Inne kluczowe systemy mediów – np. ogrzewanie/chłodzenie lub instalacje wodno-kanalizacyjne – mogą również zostać naruszone w celu zakłócenia przebiegu imprezy sportowej. Wystąpienie wymienionych sposobów ataku jest możliwe już teraz, ale prawdopodobnie ich częstotliwość zwiększy się, ponieważ systemy obiektów są coraz bardziej zdigitalizowane. Oprócz tego systemy te są w wielu przypadkach kontrolowane nie przez same obiekty, ale przez zewnętrznych wykonawców. W dobrze udokumentowanym przypadku naruszenia systemu płatności TARGET (ang. *Trans European Automated Real Time Gross Settlement Express Transfer*, Transeuropejski zautomatyzowany błyskawiczny system rozrachunku brutto w czasie rzeczywistym) hakerzy uzyskali dostęp nie za pośrednictwem systemów docelowych jako takich, ale za pośrednictwem systemów jednego z ich dostawców: sprzedawcy zdalnie sterowanych systemów HVAC (ang. *Heating, Ventilation, Air Conditioning*). Ta sama firma zajmująca się inżynierią sanitarną obsługiwała igrzyska olimpijskie w Soczi[23].

Inne potencjalne zagrożenia dla infrastruktury sportowej dotyczą wykorzystania nowych technologii w aspektach wydarzeń sportowych, takich jak oglądalność przekazów telewizyjnych z zawodów, np. podczas olimpiady w Rio używano dronów z kamerą, aby zapewnić transmisję wzdłuż torów wioślarskich[24]. (Poprzednie igrzyska olimpijskie wymagały zawieszenia kabla o długości 2 tys. m, po którym przemieszczała się kamera śledząca rywalizację łodzi). Zhakowanie dronów może spowodować poważne obrażenia fizyczne u sportowców lub widzów. W chwili obecnej technologie powstrzymujące przed atakami na drony są zaledwie w fazie rozwoju[25].

Kolejnym obszarem, który ulega cyfryzacji, jest wprowadzenie możliwości zakupu biletów na obiekty sportowe przez Internet. Coraz częściej sprzedaż wejściówek jest powiązana z mechanizmami płatności online, których można dokonać na przenośnym urządzeniu elektronicznym. Pionierskie okazały się elektroniczne opaski na rękę, które umożliwiają dostęp do obiektów, na których przebiega impreza sportowa[26]. Takie systemy będą prawdopodobnie rozwijać się w ciągu najbliższych kilku lat, ponieważ ułatwiają i przyspieszają proces płatności i identyfikacji. Ponieważ

---

[23] J. Vijayan, *Target Attack Shows Danger of Remotely Accessible HVAC Systems, Computerworld*, 7.02.2014, https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html [dostęp: 23.03.2019].

[24] J. Kanter, *Here's How the Newest Technology is Changing How We Watch the Olympics*, Business Insider, 3.08.2016, http://www.businessinsider.com/bigtv-innovations-at-rio-olympics-2016-8 [dostęp: 23.03.2019].

[25] E. Derewienko, *Systemy antydronowe coraz bardziej zaawansowane. Mają walczyć z przemytnikami*, Rynek Lotniczy, 11.09.2018, https://www.rynek-lotniczy.pl/wiadomosci/systemy-antydronowe-coraz-bardziej-zaawansowane-maja-walczyc-z-przemytnikami-4354.html [dostęp: 23.02.2019].

[26] *Chip w ręce zastąpi portfel, klucze i bilety? Chipy RFID to początek biblijnej apokalipsy?*, „Gazeta Krakowska", 14.11.2018, https://gazetakrakowska.pl/chip-w-rece-zastapi-portfel-klucze-i-bilety-chipy-rfid-to-poczatek-biblijnej-apokalipsy/ar/13664050 [dostęp: 23.03.2019].

jednak opaski, jak i inne podobne im urządzenia, konsolidują kilka potencjalnie wartościowych danych (wykorzystywanych w celu uzyskania dostępu do wydarzeń sportowych), stanowią wielką pokusę dla hakerów. Niektóre z zagrożeń są stosunkowo niewielkie; np. jeśli pojedyncza opaska zostałaby zhakowana w celu zduplikowania poświadczeń dostępu, stratę odczułby jedynie uczciwy widz, którego dostęp, z racji powtórnej próby dostania się na trybuny, mógłby zostać zablokowany. Jednak sam system obsługujący opaski może być również zhakowany w celu utrudnienia wejścia do obiektu wszystkim uczestnikom. Wystarczy wyobrazić sobie kolejkę przed ceremonią otwarcia igrzysk olimpijskich w przypadku, gdy wszystkie systemy poświadczeń dostępu jednocześnie zawiodły.

Ostanie ryzyko związane z obiektami sportowymi dotyczy systemów transportowych wykorzystywanych do przewożenia ludzi do i z miejsca imprezy. Nowoczesne samochody są coraz bardziej zdigitalizowane – w rezultacie można je hakować. Pojazdy autonomiczne – w pełni zautomatyzowane, wyposażone w technologie pozwalające systemowi wykonywać wszystkie funkcje związane z jazdą bez jakiejkolwiek interwencji ze strony człowieka, zwiększają ryzyko włamania się do systemów transportowych, głównie dlatego, że taki pojazd nie zareagowałby na zhakowane sterowanie. Zawirusowany transport, zwłaszcza gdy systemy są oparte na nielicznym zestawie dostawców, może zakłócić lub opóźnić wydarzenie sportowe. W przypadku, gdy problem z transportem dotyczy tylko kibiców, wydarzenie nadal mogłoby być rozgrywane, niestety, na podobne przeszkody mogą natrafić sportowcy, udający się na obiekty rywalizacji.

Integralność rywalizacji sportowej

Trzecia kategoria – zagrożenie cyberatakiem wpływającym na prawidłowy przebieg wydarzenia sportowego – ogranicza się do idei ruchu olimpijskiego. Czy współczesna technologia może zwiększyć prawdopodobieństwo, że w przyszłości wyniki sportowe będą kwestionowane? Poniższy fragment artykułu rozpatruje zagrożenia cybermanipulacjami w wynikach sportowych, przebiegu rywalizacji, zapisie i weryfikacji wideo oraz monitoringu sportowców.

> Pomiary sportowe i przebieg rywalizacji
>
> Sport to liczby, a liczby to wyniki pomiarów konkretnych osiągnięć w konkretnych konkurencjach. Od bezbłędnych pomiarów zależą sprawiedliwe werdykty. Natomiast bezbłędne pomiary zależą od precyzji instrumentów pomiarowych w biegach, skokach i rzutach. Mamy zatem system ogniw połączonych, w którym każde spełnia ważną funkcję. Nowe technologie zdecydowanie poprawiły parametry całego łańcucha, tworząc zupełnie nową jakość rywalizacji sportowej. Największą rolę odgrywają w dyscyplinach, w których o rezultacie decyduje zmierzony czas: pływanie, lekkoatletyka, wioślarstwo. Fotokomórki do śledzenia, który z zawodników jako pierwszy przekroczył linię mety, są coraz powszechniejsze i stanowią potencjalną lukę dla cyberprzestępców. Obecne reguły weryfikowania wyników określają, że to elektroniczny pomiar czasu jest ostatecznym, chyba że wykryje się w nim błędy[27].

[27] *FINA SWIMMING RULES 2017–2021*, Fina, ważne od 27 września 2017, https://www.fina.org/sites/default/files/2017_2021_swimming_12092017_ok_0.pdf [dostęp: 23.03.2019].

Jeszcze bardziej narażone są dyscypliny takie jak żeglarstwo czy nieolimpijskie biegi na orientację, które wykorzystują systemy GPS do monitorowania lokalizacji łodzi i zawodników[28].

Biorąc pod uwagę uważną pracę komisji skrutacyjnych zawodów oraz zapisy wideo, a także precyzyjne systemy czasowe używane w najważniejszych wydarzeniach sportowych, haker prawdopodobnie nie podjąłby się manipulowania wynikami końcowymi finałów olimpijskich. Jednak rzadziej analizowane wyniki – np. kwalifikacje do igrzysk lub zawody o mniejszej randze – mogą być łakomym kąskiem dla chociażby obstawiających w zakładach bukmacherskich.

Również dyscypliny, w których o wynikach decyduje pomiar odległości, stanowią kolejny potencjalny cel cyberataków. Weźmy pod uwagę rzut dyskiem. Chociaż historycznie odległość rzutu była mierzona za pomocą prostego sznurka lub taśmy pomiarowej, firmy takie jak FinishLynx wprowadziły laserowe systemy pomiarowe wraz z oprogramowaniem, które, jak twierdzą producenci, ma zapewnić dokładniejsze odczyty. Takie systemy pomiarowe były używane podczas mistrzostw świata[29].

RFID (ang. *Radio-frequency identification*) – technika, która wykorzystuje fale radiowe do przesyłania danych w celu identyfikacji obiektu, w chwili obecnej stanowi podstawową metodę pomiaru śledzenia wyścigów kolarskich. Chociaż do tej pory tego nie udokumentowano, należy przypuszczać, że z technologii RFID będą wkrótce korzystać konkurencje sportowe oparte na rzutach i mierzeniu odległości. Systemy używane do przesyłania i przechowywania odczytów z takich urządzeń mogą stanowić pokusę dla hakerów.

W innych sportach olimpijskich urządzenia elektroniczne nie mogą być wykorzystywane do decydowania o ostatecznych wynikach rywalizacji, niemniej jednak mogą wspierać decyzje sędziowskie, ostatecznie weryfikujące zwycięzcę. Hawk-Eye z tenisa, o którym była mowa wcześniej, jest jednym z takich przykładów. Hawk-Eye nie wskazuje zwycięzcy meczu tenisowego, ale decyduje o wyniku niektórych punktów, a gdy opinia sędziego i Hawk-Eye się różnią, decydującym będzie zapis cyfrowy.

Warto zauważyć, że również w sportach zespołowych punktacja i pomiar czasu mogą odgrywać znaczącą rolę w określaniu wyniku, np. w piłce wodnej istotnym elementem wpływającym na przebieg meczu są limity czasu posiadania piłki, których należy przestrzegać, ponieważ ich przekroczenie skutkuje rzutem karnym dla drużyny przeciwnej. Podczas igrzysk olimpijskich w 2012 r. żeńska drużyna waterpolistek Stanów Zjednoczonych błędnie wywołała przekroczenie limitu czasowego u rywalek, co doprowadziło do wskazania rzutu karnego, a w konsekwencji do dogrywki[30]. Na podobne kontrowersje narażone są inne dyscypliny wykorzystujące czas jako element

---

[28] *London 2012 Olympics: Britain's Sailors Will Be Under Same Scrutiny as Footballers During Games, Warns Sir Keith Mills*, The Telegraph, 21.02.2012, http://www.telegraph.co.uk/sport/olympics/sailing/9096214/London-2012-Olympics-Britains-sailors-will-be-under-same-scrutiny-as-footballers-during-Gameswarns-Sir-Keith-Mills.html [dostęp: 23.03.2019].

[29] LaserLynx Pro Distance Measurement, Lynx, ważne od 30 września 2017, http://www.finishlynx.com/product/event-management/laserlynx-distance-measurement/ [dostęp: 23.03.2019].

[30] B. Hamilton, *U.S. Women Overcome Coach's Error, Will Play for Water Polo Gold*, Chicago Tribune, 7.08.2012, http://articles.chicagotribune.com/2012-0807/sports/chi-us-to-play-for-gold-in-womens-water-polo-20120807_1_water-polo-gold-melissa-seidemann-adam-krikorian [dostęp: 23.03.2019].

taktyki meczu. Kto uwierzyłby trenerowi, który podczas ostatnich sekund meczu koszykarskiego powiedział, że nie nacisnął przycisku w celu wywołania przerwy w rywalizacji, skoro system elektroniczny zarejestrował, że tak zrobił?

Wreszcie, oprócz bezpośredniego wpływu na wyniki sportowe, technologia odgrywa rolę w ustalaniu, czy dany zawodnik powinien pozostać w konkurencji, czy nie. Elektroniczne połączenie bloków startowych z pistoletem startera miało ograniczyć możliwość falstartów do zera. Rozwiązanie to, niestety, budzi liczne wątpliwości, a to dlatego, że podlega ocenom mechanicznym. Ruch stopy na podstawce bloku po komendzie „Gotów" uznawany jest za falstart, chociaż sprinter nie wykonał ruchu żadną inną częścią ciała, nie sprowokował też nikogo do wcześniejszego wybiegu. W sukurs największym imprezom sportowym przyszła technologia rejestrowania falstartów[31]. Niestety, mimo że takie systemy na ogół są odłączone od Internetu w celu zmniejszenia ryzyka manipulacji, hakerzy mogą próbować je złamać i nimi manipulować w celu wywołania zbyt wczesnego startu i dyskwalifikacji.

W skokach w dal i w trójskoku najnowszym sposobem pomiarów jest system VDM (Video Distance Measurement). System odszukuje ślad w piaskownicy najbliższy linii odbicia i zarejestrowany przez aparaturę wideo. Jego zaletą jest możliwość ponownego sprawdzenia, czy odczyt był prawidłowy, czego nie zapewniał system poprzednio stosowany. Pomiar EDM (Electronic Distance Measurement), gdyż o nim mowa, nawet bez ingerencji hakerów bywa często zawodny.

Technologizacja wyników rywalizacji

W wielu przypadkach technologia nie jest stosowana do dokonywania ostatecznych pomiarów wyników rywalizacji, ale do pomocy sędziom, którzy na te wyniki mogą wpływać. Wykorzystanie technologizacji wyników na największych zawodach sportowych rośnie w zawrotnym tempie. Rozważmy przykład zdjęć z fotokomórki w lekkoatletyce: w przeciwieństwie do pływania, gdzie panel dotykowy, umieszczony na ścianie basenu, automatycznie ogłasza zwycięzcę, sędziowie w biegach lekkoatletycznych nadal zachowują kontrolę nad wynikiem. Analizie poddawane są zdjęcia z fotofiniszu, które, powtarzane i rozciągane, ujawniają, który z biegaczy torsem przekroczył linię mety. W przypadkach, gdy kilku lekkoatletów konsekwentnie ściga się na podobnym poziomie, haker może zastąpić prawdziwe zdjęcie wcześniej przygotowanym – lub całkowicie usunąć prawdziwe dane o wyścigu. Takie nieprawidłowe lub brakujące zdjęcie może zasiać wątpliwości dotyczące uznanych wyników.

Podczas zawodów pływackich igrzysk olimpijskich w Pekinie Milorad Cavic walczył z Michaelem Phelpsem. Serb przegrał minimalnie, jego federacja wniosła protest i sędziowie musieli przejrzeć dokładnie taśmę z wyścigu. Spekulacje w prasie i na blogach, kto naprawdę wygrał, trwały zdecydowanie dłużej. Aparatura jako na zwycięzcę wskazała Amerykanina, choć na zdjęciach widać, że to Cavić pierwszy dotknął ściany basenu[32]. Pływaccy notable stwierdzili wtedy: *touchpad* na ścianie basenu jest

[31] M. Jóźwik, Ślad w piaskownicy. Sędziowie tracą sporo władzy, Tygodnik TVP, 19.10.2018, https://tygodnik.tvp.pl/39479177/slad-w-piaskownicy-sedziowie-traca-sporo-wladzy [dostęp: 23.03.2019].

[32] *Cavic wyzywa Phelpsa na pojedynek 1 na 1*, Gazeta.pl, 2.08.2009, http://www.sport.pl/sport/1,65025,6886998,Cavic_wyzywa_Phelpsa_na_pojedynek_1_na_1.html [dostęp: 23.03.2019].

głównym źródłem do ustalenia zwycięzcy wyścigu, podczas gdy zdjęcia mogą być wykorzystane tylko jako materiał zapasowy[33].

Jedynym wyjątkiem od trendu korzystania z pomocy punktowych są sporty oceniane subiektywnie, takie jak gimnastyka artystyczna. Każdy układ podlega ocenie sędziów podzielonych na dwie komisje: D-technika ciała i przyboru (poprawność wykonywanych elementów) oraz E-komisja wykonania (komisja odejmuje punkty za błędy w ćwiczeniu od wyjściowych 10,00 pkt)[34]. Poza korzystaniem z prostego odtwarzania powtórek wideo, mających pomóc sędziom ocenić, w jaki sposób wykonywane są ćwiczenia, oraz systemu przewodowego służącego przesyłaniu wyników do centralnego komputera, technologia nie zmieniła znacząco sposobu oceny gimnastyki.

W ciągu następnych lat technologia może ewoluować, aby zautomatyzować obie części procesu punktacji gimnastycznej. Po pierwsze, aplikacje do analiz wideo są coraz doskonalsze i dokładniej rozróżniają różne rodzaje treści. Takie oprogramowania mogą zostać zastosowane w celu odróżnienia sekwencji ruchów gimnastyków.

Po drugie, technologie cyfrowe mogą być wykorzystywane do identyfikacji błędów zawodników; innymi słowy, mogą ocenić ćwiczenie na podstawie stopnia, w jakim ruch gimnastyczki odbiega od ideału. Sędzia gimnastyczny odejmuje punkty od oceny bazowej, na przykład za zbyt niski skok. Komputer może być lepiej ustawiony niż oko sędziego, co może być kluczowe przy porównywaniu zawodniczek. Międzynarodowa Federacja Gimnastyczna poinformowała już, że planuje wykorzystać pilotażowe oprogramowanie laserowe 3-D do wyliczania punktów podczas olimpiady w Tokio w 2020 r.[35]

Oczywiście, pojawi się wiele głosów sprzeciwu wobec wykorzystania takiego systemu. Co więcej, gimnastyka jest sportem opartym na artyzmie i (na razie) nie jest jasne, jak skomputeryzowany system punktacji mógłby to uwzględnić. Jednak zagrożenia związane z cyberbezpieczeństwem są również istotnym problemem. Ponieważ skomputeryzowany system zawierałby wiele pojedynczych matryc ruchów i kombinacji dokonywanych w bardzo krótkim czasie, haker mógłby stosunkowo łatwo zmienić niektóre wartości punktacji. Im więcej wykonywanych w krótkim czasie sekwencji ruchów, które można zmienić, tym większa szansa na manipulację i mniejsza, że jakiekolwiek zmiany zostaną wykryte.

Jeśli kwestionowane byłyby wyniki regulowane przez punktację opartą na oprogramowaniu, bardzo trudno byłoby później przywrócić zaufanie do wiarygodności systemu. W skoku przez stół gimnastyczny, nazywanym również skokiem przez konia, podczas olimpiady w Sydney w 2000 r., kiedy aparaturę ustawiono na niewłaściwą wysokość, organizatorzy potrzebowali jedynie dostosować wysokość stołu, żeby przywrócić jego właściwe ustawienie. Jednak gdyby skompromitowano

---

[33] Associated Press, *Omega Releases Official Photos of 100-Meter Butterfly Finish*, ESPN.com, 23.08.2008, http://www.espn.com/olympics/summer08/swimming/news/story?id=3550164 [dostęp: 23.03.2019].

[34] *Przepisy i regulaminy*, Polski Związek Gimnastyczny, https://pzg.pl/gimnastyka-artystyczna/przepisy-i-regulaminy/, [dostęp: 23.03.2019].

[35] J. Grassie, *3D Lasers to be Part of Gymnastics Judging at 2020 Tokyo Olympics*, NBC Olympics, 18.05.2016, http://www.nbcolympics.com/news/3-d-lasers-bepart-gymnastics-judging-2020-tokyo-olympics [dostęp: 23.03.2019].

sam elektroniczny system oceniania, prawie niemożliwe byłoby wykrycie tego, co się stało, oraz – naprawa.

Monitoring sportowca

Dotychczasowa analiza skoncentrowana była na działaniach mających na celu zmodyfikowanie wyników rywalizacji sportowej, bezpośrednio lub poprzez wpływ na decyzje sędziów. Istnieją jednak inne sposoby, gdzie brak wystarczającego bezpieczeństwa cybernetycznego może zagrozić integralności ważnych wydarzeń sportowych: ingerencja w metody poprawiania wydolności organizmów sportowców, ale również *biohacking* – sprowadzający się do traktowania ludzkiego ciała niczym urządzenia.

W dotychczas opisywanych przykładach nie został poruszony problem cyberzagrożeń, które mogłyby bezpośrednio wpłynąć na poprawę/pogorszenie wyników sportowców podczas startu na zawodach sportowych (chociaż zidentyfikowano sposoby, jakimi sportowcy mogą teoretycznie oszukiwać przy użyciu technologii, np. pływak może nosić elektroniczne urządzenie, które pomogłoby mu śledzić i utrzymywać właściwe tempo). Istnieją jednak metody, za pomocą których haker może wpływać na wyniki zawodników w samym procesie przygotowań do zawodów: manipulując suplementami spożywanymi przez sportowców, ale również szeroko rozumianą opieką medyczną.

Zautomatyzowane systemy żywieniowe stają się coraz powszechniejsze. Sportowcy, którzy starannie regulują spożycie pokarmów, zdają sobie sprawę, że ich systemy żywienia odgrywają ważną rolę w przygotowaniach do zawodów, przykładem koktajle proteinowe: Produkty te różnią się od siebie choćby ilością zawartego białka[36], dzięki czemu sportowcy mogą dostosowywać spożycie do szczegółowych specyfikacji dietetyków. Wystarczy sobie wyobrazić zhakowanie systemu dozującego składniki shake'ów proteinowych przygotowywanych dla dużych zespołów sportowców.

Zautomatyzowane systemy stwarzają niebywałą okazję dla hakerów chcących zakłócić wyniki sportowe. Hipotetyczny przykład: biegacz z alergią na gluten, każdego dnia przed treningiem spożywający koktajl proteinowy. Ekipa jego najgroźniejszego rywala włamuje się do automatycznego systemu dozowania białek, sprawiając, że gluten zostanie podany do napoju. Oszukany biegacz nie osiągnie najwyższej wydajności – i być może, w ogóle nie będzie w stanie przystąpić do rywalizacji.

Z kolei „ulepszanie" człowieka przez *biohacking*, czyli wszczepiane chipy, cyfrowe tatuaże, bioniczne protezy, a nawet modyfikacje DNA, ma prowadzić do zwiększania komfortu sportowca, poprawy jego możliwości, usuwania cielesnych defektów, a nawet do długowieczności. Nie jest to wcale nowe zjawisko – ludzie na różne sposoby hakowali swoje ciała od dawna. Zwykły człowiek ma opór przed takimi rozwiązaniami, które naruszają cielesną integralność, lecz sportowcy, dla olimpijskiej glorii, mogą być skłonni wpuścić do swoich organizmów np. nanoroboty. A te mogą w przyszłości zastąpić medycynę konwencjonalną i „usprawniać" w sposób celowany wybrane narządy. Najnowsze osiągnięcia pozwalają np. na edycję DNA. Taka technologia umożliwi modyfikację genów. Ale rodzi też liczne zagrożenia.

[36] E. Jed, *Weider Vending Machine Delivers Freshly Blended Protein Shakes*, Vending Times, 8.06.2015, https://www.vendingtimes.com/main/articles/5859.aspx [dostęp: 23.03.2019].

Przykład? Dwa lata temu naukowcy University of Washington w ramach eksperymentu zakodowali w nici DNA cyfrowego wirusa[37]. W ten sposób włamali się do komputera, który analizował próbkę. W przypadku wszczepianych chipów rodzi się zaś pytanie o inwigilację ich nosicieli oraz ochronę takich osób przed cyperprzestępcami. W przyszłości hakerzy będą mogli bowiem nie tylko wykradać dane z implantów, ale również wpływać na zachowanie ludzi, których mózgi czy mięśnie wspomagają wszczepione technologie.

Ryzyko finansowe

Każde z dotychczas opisanych zagrożeń, oprócz zakłócenia integralności sportu i infrastruktury, w których sport ten jest uprawiany, może mieć poważne reperkusje finansowe. Ponadto niektóre potencjalne ataki są bezpośrednio ukierunkowane na zyski finansowe. Niektóre z tych zagrożeń, takie jak fałszywe witryny internetowe i oszustwa biletowe, są już dobrze znane. Prawdopodobnie będą występować w przyszłości, ale jest mało prawdopodobne, by ich mechanizmy znacząco się zmieniły.

Można również zidentyfikować kilka innych wektorów dodatkowego ryzyka finansowego. Jednym z takich zagrożeń jest tendencja systemów elektronicznych do łączenia pożądanych aktywów w jeden system. Jednym z przykładów są skonsolidowane systemy płatności i biletowania odnotowane wcześniej. Oprócz już opisanego ryzyka takie systemy mogą być wykorzystywane do gromadzenia skomasowanych danych finansowych klientów. Ponieważ każdy uczestnik będzie musiał korzystać z opaski, na której będzie zapisany jego bilet, jeśli system zostanie zainfekowany, hakerom łatwiej będzie zbierać szczegóły płatności od wszystkich użytkowników opasek jednocześnie. Obecnie groźba cyberprzestępstwa ogranicza się do osób korzystających z elektronicznych metod płatności za bilety, a ryzyko zmienia się w zależności od rodzaju zastosowanej płatności.

Ryzyko strategiczne i reputacyjne

Ostatnim rodzajem cyberbezagrożeń jest ryzyko potencjalnie negatywnego rozgłosu w mediach: nawet bez powodowania szkód fizycznych lub finansowych hakerzy mogą negatywnie wpłynąć na wizerunek zawodów sportowych. W przypadku dużych wydarzeń jednym z istotnych obszarów zainteresowania, prowadzonym przez organizatorów polityki prestiżu, jest wizerunek imprezy wśród opinii publicznej zgromadzonej przed telewizorami. Działania hakerskie na obiektach sportowych, o ile nie są transmitowane szerzej, dotyczą osób zgromadzonych na obiekcie. Jednak możliwość dotarcia ze sportowymi emocjami do milionów ludzi w domowych zaciszach daje idei olimpijskiej ogromny zasięg. Dla przykładu, jeśli haker umieścił nieprzyzwoite treści na tablicy świetlnej stadionu, wpłynęłoby to tylko na obecnych w danym miejscu i czasie – przynajmniej, dopóki ktoś z widzów nie umieściłby ich na Twitterze.

[37] M. Duszczuk, *Biohacking, czyli początek ery cyborgów*, Rzeczpospolita, 25.03.2019, https://cyfrowa.rp.pl/technologie/32757-hakowanie-cial-oto-zaczyna-sie-era-cyborgow, [dostęp: 25.03.2019].

W miarę jak zmieniają się preferencje oglądania najważniejszych wydarzeń sportowych, hakerzy będą mogli wpływać na to, czego widzowie doświadczają. W niedługim czasie wirtualna rzeczywistość zapewni kolejne wspaniałe wrażenia wizualne, pozwalając widzom prawie dosłownie „wejść w buty" sportowca. Ponieważ systemy oparte na 3D umożliwiają widzom obserwację z wielu perspektyw jednocześnie, będzie bardzo trudno zorientować się, kiedy na ekranie pojawi się coś niewłaściwego. W przypadku jednego kanału telewizyjnego producent zawsze może szybko zareagować, gdy coś pójdzie nie tak; z setkami lub tysiącami symultanicznych obrazów w technologii wideo 360° wyłapanie niepożądanych treści będzie o wiele trudniejsze.

Podsumowanie

Chociaż istniejące zagrożenia bezpieczeństwa cybernetycznego – koncentrujące się głównie w kategorii ryzyka finansowego – prawdopodobnie będą się utrzymywać, pojawią się również nowe metody cyberataków. Przyszłe ataki będą trudniejsze do przeprowadzenia, ale i konsekwencje dla wydarzeń sportowych będą poważniejsze.

Jeszcze jedną kategorią ryzyka związanego z cyberzagrożeniami jest ich wykrywalność. W niektórych przypadkach hakerzy chcą, aby ich „dzieło" miało skutek natychmiastowy (tak jak w przypadku ataku przeprowadzonego podczas rozgrywek sportowych lub opublikowania skradzionych danych), lub dlatego, że w niektórych przypadkach same efekty ataku (atak terrorystyczny lub porwanie) sprawią, że odkrycie cyberataku będzie mało prawdopodobne.

Najtrudniejsze do wykrycia cyberataki koncentrują się na „integralności sportu". W miarę postępu cyfryzacji dużych dyscyplin sportowych coraz trudniej będzie stwierdzić, czy cyberatak wpłynął na wynik ważnego wydarzenia sportowego – może nawet trudniej niż wykrycie nieuczciwych transakcji finansowych. W rezultacie ilość korzyści skłaniających hakerów do cyberprzestępstw będzie rosła.

Zalecenia i wnioski

Do tej pory cyberbezpieczeństwo sportu nie było uważane za istotny temat badań naukowych. Niniejszy artykuł jest tylko wstępem do dyskusji nie tylko o cyberbezpieczeństwie największych imprez sportowych, ale również wszelkich innych masowych wydarzeń, zmieniających swój charakter z analogowych na cyfrowe.

W istocie sporty olimpijskie (i prawdopodobnie również inne wydarzenia sportowe) są narażone na niemal wszystkie typy cyberzagrożeń. Z jednej strony ważnym celem zarządzania cyberbezpieczeństwem jest minimalizacja zagrożeń, z drugiej – eliminacja ich wszystkich nie jest możliwa. W wirtualnej przestrzeni zawsze znajdą się niebezpieczne luki, a osoby odpowiedzialne za zapewnienie cyberbezpieczeństwa dużych wydarzeń sportowych będą zmuszone ustalić priorytety w przypadku wystąpienia kryzysu, aby sprostać szerokiemu zakresowi zagrożeń, przed którymi staną.

W 2016 r. eksperci z Kaspersky Lab dokładnie przeanalizowali pięć największych zagrożeń internetowych, z jakimi borykały się igrzyska w Rio[38]. Główne zagrożenia do-

[38] K. Kochetkova, *op. cit*.

tyczyły: list phishingowych i fałszywych strony, zhakowanych sieci wi-fi, skimmerów kart bankomatowych oraz fałszywych bankomatów.

Dziś ta lista wyglądałaby inaczej. Niniejsze artykuł definiuje osiem kluczowych obszarów zagrożeń, które powinny mieć pierwszeństwo przed innymi ze względu na swą szkodliwość:

- hakowanie infrastruktury obiektów fizycznych;
- hakowanie systemu punktacji sportowej;
- hakowanie powtórek zapisów wideo i fotofiniszów;
- *biohacking*;
- hakowanie systemów wejść na obiekty sportowe;
- hakowanie systemu transportowego;
- hakowanie w celu ułatwienia terroryzmu lub porwania;
- hakowanie wywołujące panikę.

Co więcej, ze względu na niską wykrywalność ataki wpływające na uczciwość gry (punktacja, powtórki zapisów wideo i *biohacking*) są szczególnie warte uwagi.

Jedną z lekcji, jaką powinni odrobić organizatorzy imprez sportowych, jest potrzeba zrównoważenia szansy i ryzyka. Pokusa unowocześniania sportu poprzez nowe technologie jest ogromna, należy się jednak zastanowić, czy gra warta jest świeczki. Decyzja o przyjęciu nowej technologii, zwłaszcza gdy w grę wchodzi nieśmiertelna chwała zwycięzców igrzysk olimpijskich, powinna być zawsze podejmowana z uwzględnieniem potencjalnego ryzyka cyberbezpieczeństwa.

Czasem wystarczą proste, standardowe zabezpieczenia, jak osłony ekranów komputerów, na których wpisywane są hasła dostępu do poufnych danych. W ten sposób można uniknąć wzroku przypadkowych osób, które mogłyby włamać się do komputera. Wszystkie komputery wykorzystywane podczas wydarzeń sportowych powinny używać uwierzytelniania wieloczynnikowego w celu ograniczenia dostępu, a hasła nigdy nie powinny być wpisywane na oczach widzów.

Oficjele sportowi muszą również zadbać, aby wszelkie nowe technologie wykorzystywały komputery znajdujące się w fizycznie odizolowanych od Internetu sieciach, tzw. *air-gapped networks*. W coraz bardziej cyfrowym świecie przeżytkiem może się wydawać korzystanie z przewodów, ale to właśnie sieci przewodowe zniechęcają przestępców, którym dużo łatwiej przychodzi hakowanie sieci bezprzewodowych.

Kolejną kluczową zasadą powinna być duplikacja: każde urządzenie cyfrowe używane podczas imprezy musi mieć kopię zapasową w przypadku awarii, a odpowiednie osoby powinny zapewnić nadzór w celu sprawdzenia, czy jakakolwiek technologia cyfrowa wykorzystywana w zawodach sportowych daje rzetelny wynik. Proste, manualne stopery powinny być wykorzystywane jako uzupełnienie elektronicznych pomiarów. Zdjęcia fotofiniszów powinny być sprawdzane przez sędziów, a nie tylko przez komputer. Dane wprowadzane do elektronicznych systemów umożliwiających rozstrzygnięcie kontrowersyjnych punktów, takich jak Hawk-Eye, powinny być walidowane pod kątem dokładności. Choć duplikowanie może się wydawać niepotrzebnym procesem – w ogromnej większości przypadków sprzęt cyfrowy okaże się wystarczający – będzie idealnym rozwiązaniem w przypadku wystąpienia cyberzagrożeń kwestionujących uczciwość rywalizacji sportowej.

Cyberbezpieczeństwo jest często postrzegane wyłącznie jako domena specjalistów IT. Jednak każda osoba – od sprzedawców biletów, elektryków, trenerów,

kierowników obiektów, po widzów – ma do odegrania ważną rolę w zachowaniu cyberbezpieczeństwa podczas imprezy sportowej. Wszyscy są narażeni są na potencjalne ryzyko związane z awarią systemów cyfrowych . Każdy uczestnik imprezy sportowej – czy to aktywny, czy bierny – powinien poszerzyć wiedzę na temat tego, kogo dotyczy cyberbezpieczeństwo najważniejszych wydarzeń sportowych. Idąc tym tropem – cyberbezpieczeństwo dotyczy prawdopodobnie wszystkich.

Bibliografia

Associated Press, *Omega Releases Official Photos of 100-Meter Butterfly Finish*, ESPN.com, 23.08.2008, http://www.espn.com/olympics/summer08/swimming/news/story?id=3550164 [dostęp: 23.03.2019].

Bisson D., *How A Massive 540 Gb/Sec DDoS Attack Failed to Spoil the Rio Olympics*, Tripwire, 5.09.2016, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/how-a-massive-540-gbsec-ddos-attack-failed-to-spoil-the-rio-olympics/ [dostęp: 27.03.2019].

Brill A., Petreska S., *Are Cyber Criminals Competing at the Olympics?*, Freedom From Fear Magazine, 24.05.2016, http://insct.syr.edu/wp-content/%20uploads/2015/05/Brill_Olympics.pdf [dostęp: 23.03.2019].

Burton ZG., *How the London Olympics Dealt With Six Major Cyber Attacks*, Computing, 6.03.2013, https://www.computing.co.uk/ctg/news/2252841/howthe-london-olympics-dealt-with-six-major-cyber-attacks#comment_form [dostęp: 23.03.2019].

Cavic wyzywa Phelpsa na pojedynek 1 na 1, Gazeta.pl, 2.08.2009, http://www.sport.pl/sport/1,65025,6886998,Cavic_wyzywa_Phelpsa_na_pojedynek_1_na_1.html [dostęp: 23.03.2019].

Chip w ręce zastąpi portfel, klucze i bilety? Chipy RFID to początek biblijnej apokalipsy?, „Gazeta Krakowska", 14.11.2018, https://gazetakrakowska.pl/chip-w-rece-zastapi-portfel-klucze-i-bilety-chipy-rfid-to-poczatek-biblijnej-apokalipsy/ar/13664050 [dostęp: 23.03.2019].

Corera G., The 'Cyber-Attack' Threat to London's Opening Ceremony, BBC News, 8.07.2013, http://www.bbc.com/news/uk-23195283 [dostęp: 23.03.2019].

Cyberbezpieczeństwo na arenach sportowych, 4safe.pl, 15.09.2016, http://www.4safe.pl/wiadomosci/10/cyberbezpieczenstwo_na_arenach_sportowych [dostęp: 27.03.2019].

Cyberbezpieczeństwo na międzynarodowych imprezach sportowych, takich jak Mistrzostwa Świata w Piłce Nożnej 2018, itd24.pl, 18.07.2018, https://itd24.pl/quick-heal-seqrite/cyberbezpieczenstwo-na-miedzynarodowych-imprezach-sportowych-takich-jak-mistrzostwa-swiata-w-pilce-noznej-2018/ [dostęp: 27.03.2019].

Derewienko E., *Systemy antydronowe coraz bardziej zaawansowane. Mają walczyć z przemytnikami*, Rynek Lotniczy, 11.09.2018, https://www.rynek-lotniczy.pl/wiadomosci/systemy-antydronowe-coraz-bardziej-zaawansowane-maja-walczyc-z-przemytnikami-4354.html [dostęp: 23.02.2019].

Duszczuk M., *Biohacking, czyli początek ery cyborgów*, Rzeczpospolita, 25.03.2019, https://cyfrowa.rp.pl/technologie/32757-hakowanie-cial-oto-zaczyna-sie-era-cyborgow, [dostęp: 25.03.2019].

Grassie J., *3D Lasers to be Part of Gymnastics Judging at 2020 Tokyo Olympics*, NBC Olympics, 18.05.2016, http://www.nbcolympics.com/news/3-d-lasers-bepart-gymnastics-judging-2020-tokyo-olympics [dostęp: 23.03.2019].

Guerrini F., *Brazil's World Cup of Cyber Attacks: From Street Fighting to Online Protest*, Forbes, 17.06.2014, https://www.forbes.com/sites/federicoguerrini/2014/06/17/brazils-world-cup-of-cyber-attacks-from-street-fighting-to-online-protest/#49874ca251a8 [dostęp: 27.03.2019].

Hacked within Minutes: Sochi Visitors Face Internet Minefield, NBC News, 4.02.2014, http://www.nbcnews.com/video/nightly-news/54273832#54273832 [dostęp: 23.03.2019].

Hamilton B., *U.S. Women Overcome Coach's Error, Will Play for Water Polo Gold*, Chicago Tribune, 7.08.2012, http://articles.chicagotribune.com/2012-0807/sports/chi-us-to-play--for-gold-in-womens-water-polo-20120807_1_water-polo-gold-melissa-seidemann--adam-krikorian [dostęp: 23.03.2019].

Hampshire J., *Professional Sports Teams Are Risking a Cybersecurity Own Goal*, Infosecurity Group, 11.08.2015, https://www.infosecurity-magazine.com/opinions/professional--sports-teams/ [dostęp: 27.03.2019].

Jed E., *Weider Vending Machine Delivers Freshly Blended Protein Shakes*, Vending Times, 8.06.2015, https://www.vendingtimes.com/main/articles/5859.aspx [dostęp: 23.03.2019].

Jóźwik M., *Ślad w piaskownicy. Sędziowie tracą sporo władzy*, Tygodnik TVP, 19.10.2018, https://tygodnik.tvp.pl/39479177/slad-w-piaskownicy-sedziowie-traca-sporo-wladzy [dostęp: 23.03.2019].

Kanter J., *Here's How the Newest Technology is Changing How We Watch the Olympics*, Business Insider, 3.08.2016, http://www.businessinsider.com/bigtv-innovations-at-rio-olympics-2016-8 [dostęp: 23.03.2019].

Kaplan J.A., *NBC News Takes Heat over Sochi Phone Hacking Report*, Fox News, 7.02.2014, http://www.foxnews.com/tech/2014/02/07/nbc-news-takesheat-over-sochi-phone-hacking-report.html [dostęp: 23.03.2019].

Kochetkova K., *Trendy w cyberzagrożeniach podczas Igrzysk Olimpijskich*, Kaspersky Lab, 19.07.2016, https://plblog.kaspersky.com/olympic-games-2016-threats-guide/5152/ [dostęp: 27.03.2019].

Lider Tour de France zaatakowany przez hakerów!, Fakt24, 15.07.2015, https://www.fakt.pl/sport/inne-sporty/hakerzy-przypuscili-atak-na-lider-tdf-chrisa-frooma/xexweqr [dostęp: 23.04.2019].

London 2012 Olympics: Britain's Sailors Will Be Under Same Scrutiny as Footballers During Games, Warns Sir Keith Mills, The Telegraph, 21.02.2012, http://www.telegraph.co.uk/sport/olympics/sailing/9096214/London-2012-Olympics-Britains-sailors-will-be-under-same-scrutiny-as-footballers-during-Gameswarns-Sir-Keith-Mills.html [dostęp: 23.03.2019].

Nowak A., *Anonymous zaatakowali strony Formuły 1*, „Bezpieczeństwo. Dziennik Internautów", 23.04.2012, http://di.com.pl/anonymous-zaatakowali-strony-formuly-1-44876 [dostęp: 27.03.2019].

Pells E., *Gymnastics: Olympic Vault Set Too Low*, ABC News, http://abcnews.go.com/Sports/story?id=100494&page=1 [dostęp: 27.03.2019].

Rosyjscy hakerzy wykradli dane medyczne sportsmenek z Rio, Wprost, 13.09.2016, https://www.wprost.pl/sport/10023047/Rosyjscy-hakerzy-wykradli-dane-medyczne-sportsmenek-z-Rio.html [dostęp: 23.03.2019].

Rumsby B., *Rugby World Cup 2015 Tickets: Cyber Criminals Plotting to Hijack Launch*, The Telegraph, 11.09.2014, http://www.telegraph.co.uk/sport/rugbyunion/

rugby-world-cup/11088098/Rugby-World-Cup-2015-tickets-Cyber-criminals-plotting-to-hijack-launch.html [dostęp: 23.03.2019].

Securing the 2012 Olympics, Infosecurity Group, 19.11.2009, https://www.infosecurity-magazine.com/magazine-features/securing-the-2012-olympics [dostęp: 27.03.2019].

Stinson S., *If Leagues Decide Gambling Can Help Grow Their Games, Trump Could Help Deliver*, National Post, 4.03.2017, https://nationalpost.com/sports/if-leagues-decide-gambling-can-help-grow-their-games-trump-could-help-deliver [dostęp: 27.03.2019].

Vijayan J., *Target Attack Shows Danger of Remotely Accessible HVAC Systems, Computerworld*, 7.02.2014, https://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html [dostęp: 23.03.2019].

Wawak S., TurekB., *Analiza FMEA*, Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Analiza_FMEA, [dostęp: 27.03.2019].

Więcej złośliwego oprogramowania podczas Olimpiady 2012, WebSecurity, 6.08.2012, http://websecurity.pl/tag/olimpiada [dostęp: 23.03.2019].

Zobacz, jakie ataki szykują hakerzy na igrzyska olimpijskie, eGospodarka.pl, 18.02.2018, http://www.egospodarka.pl/146729,Zobacz-jakie-ataki-szykuja-hakerzy-na-igrzyska-olimpijskie,1,12,1.html [dostęp: 27.03.2019].

Wielkie imprezy sportowe a nowe technologie: trendy w cyberzagrożeniach
Streszczenie

Artykuł omawia specyficzne cyberzagrożenia występujące podczas przygotowań do wielkich imprez sportowych i ich trwania. Przyjmując Igrzyska Olimpijskie za studium przypadku, wskazuje potencjalne niebezpieczeństwa stwarzane przez technologie cyfrowe wykorzystywane w sporcie i przewiduje nowe możliwe zagrożenia, które pojawią się w miarę wdrażania tych technologii. Podano szeroką gamę ryzyka: od bezpośredniego wpływu na przebieg rywalizacji sportowej po odbiór imprezy przez kibiców. Na koniec przedstawiono propozycje walki z cyberzagrożeniami.

Słowa kluczowe: cyberbezpieczeństwo, cyberzagrożenia, igrzyska olimpijskie, sport

Mega-Sporting Events and New Technologies: Trends in Cyber Threats
Abstract

The paper looks at the specific cyber threats that occur during the preparation of major sports events and in the course of such events. By taking the Olympic Games as a case study, it indicates the potential dangers posed by digital technologies used in sports and anticipates new possible threats that will arise as these technologies are implemented. A wide range of risks has been given: from direct impact on the course of sports competition to the reception of the event by the fans. Finally, proposals for combating cyber threats are presented.

Key words: cybersecurity, cyber threats, Olympic Games, sport

Maciej Saskowski

Große Sportveranstaltungen und neue Technologien: Trends in Cyber- Bedrohungen
Zusammenfassung

Der Artikel bespricht spezifische Cyberrisiken, welche während der Vorbereitungen der großen Sportveranstaltungen und während ihrer Laufzeit auftreten. Er nimmt die Olympischen Spiele als Fallstudium an und nennt die potenziellen Gefahren, welche die im Sport genutzten Cybertechnologien schaffen und sieht neue mögliche Risiken vor, die bei der Anwendung dieser Technologien auftreten können. Es wurde eine breite Palette von Risiken angeführt: vom direkten Einfluss auf den Verlauf des Sport-Wettkampfs bis zur Entgegennahme der Veranstaltung durch die Sportfans. Am Ende wurden Vorschläge zur Bekämpfung der Cyber-Bedrohungen gemacht.
Schlüsselwörter: Cybersicherheit, Cyberrisiken, Olympische Spiele, Sport

Большие спортивные события и новые технологии: тенденции киберугроз
Резюме

В статье рассматриваются специфические киберугрозы, возникающие во время подготовке и проведения больших спортивных событий. Рассматривая Олимпийские игры в качестве тематического исследования, автор указывает на такие потенциальные опасности, какими являются используемые в спорте цифровые технологии, и предвидит новые угрозы, которые будут возникать по мере внедрения этих технологий. Автор приводит широкий спектр рисков, непосредственно влияющих на ход спортивных соревнований и связанных с отношением к мероприятию болельщиков, представляет предложения по борьбе с киберугрозами.
Ключевые слова: кибербезопасность, киберугрозы, Олимпийские игры, спорт