ceis

JANVIER 2018

SECURITE DES GRANDS EVENEMENTS SPORTIFS

Vincent Riou, Directeur Cybersécurité, CEIS
Ilona Ignatova, Consultante Cyber Risques, CEIS

Les notes stratégiques

L'INTELLIGENCE DE LA DÉCISION

LES NOTES STRATÉGIQUES

Notes d'étude et d'analyse

SecuInsight, l'offre de Cyber Threat Intelligence de CEIS, permet d'analyser l'ensemble des risques cyber externes des entreprises par des recherches ciblées sur les clear, deep et dark web (fuites de données, vulnérabilités apparentes, revendications d'attaques sur les media sociaux, fraudes…), et d'élaborer des scénarios anticipatifs de crise dans le but de préparer efficacement les défenses techniques et humaines.

CEIS dispose de plus de 15 ans d'expérience dans le management des risques liés au monde du sport et est le prestataire de Cyber Threat Intelligence du Comité d'Organisation d'un événement sportif de portée mondiale.

Les auteurs :
Vincent Riou dirige la business unit cybersécurité de CEIS.
Ilona Ignatova est consultante en cyber risques dans l'équipe « SecuInsight » de CEIS.

TABLE DES MATIÈRES

1. EVÈNEMENTS SPORTIFS ET NOUVELLES TECHNOLOGIES : OPPORTUNITÉS ET MENACES 4

2. HISTORIQUE 6

3. ANALYSE DES MOTIVATIONS 9

4. IDENTIFICATION DES RISQUES MAJEURS 11

4.1 Actions visant l'organisation de l'évènement 11

4.2 Actions visant les délégations et les sportifs 15

4.3 Actions visant le business du sport 16

4.4 Actions visant les systèmes de l'Etat hôte 17

5. TABLEAU DE SYNTHÈSE 19

6. RECOMMANDATIONS 22

1. EVÈNEMENTS SPORTIFS ET NOUVELLES TECHNOLOGIES : OPPORTUNITÉS ET MENACES

Les grands évènements sportifs sont extrêmement populaires. Attendus par des populations de supporters du monde entier, ils cristallisent les passions et génèrent un business de plusieurs centaines de milliards d'euros tous les ans.

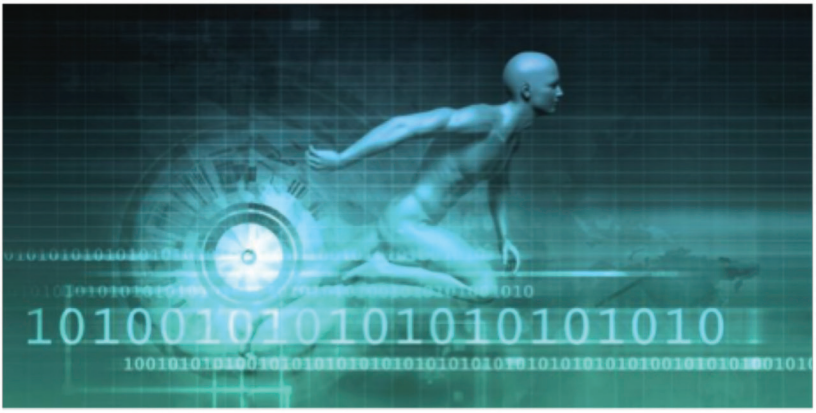
Les tentations des criminels, activistes et terroristes sont exacerbées par la portée de ces évènements. Les premiers souhaiteront prendre une part de cet énorme gâteau, les seconds en profiteront pour tenter de porter leurs messages idéologiques à la planète entière et les derniers y verront un terrain idéal pour y mener leurs actions : foules compactes, retentissement maximal.

La numérisation du sport est une formidable opportunité. Les nouvelles technologies améliorent les performances et l'entraînement des athlètes, améliorent l'expérience sensorielle des spectateurs et aident aux décisions des juges et arbitres.

Cependant, chaque nouvelle opportunité apporte son lot de nouvelles menaces. Ces technologies numériques, objets connectés, systèmes industriels, systèmes temps réels, présentent tous une inéluctable surface de vulnérabilité, souvent favorisée par une hyper-connexion à Internet.

«*Si je devais choisir un seul défi, ce serait celui de la sécurité. Il y a de nombreuses menaces terroristes à travers le monde. Il ne s'agit pas uniquement d'une menace physique, mais aussi d'une menace de cyberterrorisme*» déclarait au journal Japan Times, en avril dernier, Toshiro Muto, Directeur Général du Comité d'organisation des Jeux Olympiques de Tokyo en 2020. Ainsi, le ministère de l'Intérieur et des Communications japonais a lancé un plan de mesures d'environ 150 millions d'euros pour la cybersécurité sur la période 2016-2020.

A l'approche des grands évènements qu'accueillera la France en 2023 et 2024, cette note stratégique a pour objectif de favoriser la réflexion autour des risques cyber pesant sur les grands tournois et compétitions majeurs. Il n'est pire politique de sécurité que de se croire en sécurité. Connaître la menace, l'anticiper, est indispensable pour mieux s'en prémunir. Il ne faut donc pas voir dans cette note une vision pessimiste de l'avenir, mais une opportunité de réagir en amont pour prévenir ces risques.



2. HISTORIQUE

Pour donner au lecteur une idée de la menace et de sa portée, faisons tout d'abord un rapide retour sur les attaques constatées lors des grands évènements sportif de ces dernières années.

Atos, qui fournit l'infrastructure informatique des JO depuis 1992, a répertorié plus de 12 millions d'attaques par jour lors des Jeux Olympiques de Pékin en 2008, dont 420 évènements à risque. Lors des JO de Londres, 212 millions de connections frauduleuses ont été détectées. De même, 200 évènements à risque ont été détectés et traités lors des JO d'hiver à Sotchi en 2012. Les attaques sont larges, de la tentative d'obtention de données confidentielles sur les athlètes au blocage du système de diffusion des résultats.

La Coupe du Monde de Football au Brésil en 2014 a été le théâtre d'une large gamme d'attaques informatique, en intensité et en diversité. Des hacktivistes ont réussi à voler puis diffuser des données confidentielles du ministère des affaires étrangères, et ont lancé de très nombreuses attaques en déni de service (DDoS). Les Anonymous, entre autres, ont lancé des dizaines d'attaques DDoS ou de défiguration de sites Web afin de protester contre la corruption et l'injustice économique constatées dans le pays. Des bases de données liées à l'événement ont aussi été diffusées (comme celle du site copa2014.df.gov.br), ainsi que 450 comptes mails avec mots de passe de membres du gouvernement brésilien. Côté cybercriminalité, on a pu répertorier de nombreuses attaques sur les distributeurs de billets de banque, du trafic de téléphones portables, de la fraude sur les billets d'accès au stade, de faux sites de pari sportif… Et cela s'est largement poursuivi deux ans plus tard lors des JO de Rio, avec de nombreux ransomwares téléchargés par le biais de sites sensés présenter les résultats des compétitions, de larges campagnes de phishing ciblées, la compromission de spots Wifi non sécurisés permettant l'injection de chevaux de Troie bancaires, l'une des spécialités locales.

Plus récemment, le groupe de hackers russes Fancy Bears a dévoilé une liste de footballeurs ayant bénéficiés d'une autorisation d'usage de produits à des fins thérapeutiques pendant la Coupe du Monde 2010 en Afrique du Sud, déclarant dans leur communiqué que « *les joueurs et les officiels affirment de manière unanime que ce sport n'est pas touché par le dopage. Notre équipe a pris ces nombreuses déclarations pour un défi et va désormais prouver que ce sont des mensonges.* »

En 2016, ces hackers russes avaient déjà fait fuiter les données médicales d'une trentaine d'athlètes, dont celles des sœurs Williams.

Alors que la Russie se voit privée de participation aux Jeux Olympiques d'hiver 2018 en Corée du Sud, il y a fort à parier que des actes similaires se multiplieront dans les prochains mois…

3. ANALYSE DES MOTIVATIONS

CYBERCRIMINALITÉ

L'augmentation du volume de transactions financières liées à un grand événement sportif est un vecteur d'attraction pour les cybercriminels. De nombreux supporters, lors des compétitions, vivent une forme d'insouciance facilitant les arnaques en tout genre, dans le cyberespace comme dans la vie réelle. Dans le cas de ransomwares visant des entreprises travaillant au succès de l'évènement, il est également évident qu'elles seront plus enclines à payer, au vu des enjeux calendaires et politiques liées au succès de celui-ci.

HACKTIVISME

Le retentissement médiatique mondial d'un grand événement sportif, ainsi que la notoriété des sportifs de haut niveau fait l'effet d'une caisse de résonnance pour les différentes idéologies véhiculées par les hacktivistes. Ainsi, comme au Brésil en 2014 et 2016, les revendications de ceux-ci n'étaient pas sportives mais bien politiques. Le sport n'est ici qu'un support à l'expression de contestations politiques ou sociétales.

CYBERGUERRE

Lorsqu'un Etat organise les JO ou une Coupe du Monde, il focalise l'attention de ses ennemis idéologiques, politiques ou économiques. On peut imaginer dès lors que certains Etats voient en l'échec de la compétition un moyen de déstabilisation du pays visé. Ainsi, le Qatar, pour l'organisation de la future Coupe du Monde de la FIFA en 2022, est déjà la cible d'Etats rivaux. Et si la Corée du Sud, organisatrice des JO d'hiver 2018, a récemment autorisé la venue d'une délégation de sportifs nord-coréens, c'est vraisemblablement aussi pour limiter les risques de sabotage de la compétition par voie numérique, les hackers de ce pays étant particulièrement compétents et motivés. Ceux-ci l'ont largement prouvé en septembre 2016 lorsqu'ils ont volé plus de 235 Go de données confidentielles à l'armée sud-coréenne, dont le plan opérationel 5015, le dernier plan d'action américano-sud-coréen conçu dans l'éventualité d'une guerre avec le Nord et qui comporte notamment des projets d'attaques pour supprimer le dirigeant nord-coréen Kim Jong-un.

CYBER-TERRORISME

La menace terroriste pèse sur tout événement international. Comme nous le verrons dans ce document, elle peut être facilitée par des actions dans le cyberespace. Des délégations de certains pays peuvent être visées. L'image du massacre de 11 membres de la délégation israélienne lors des JO de Munich en 1972 est encore dans tous les esprits. Plus récemment, des menaces de Daesh ont été proférées avant les JO de Rio. Les autorités ont pris la menace très au sérieux, car même si le Brésil, qui ne fait pas partie de la coalition internationale luttant contre Daesh en Syrie et en Irak, n'est pas une cible évidente, un événement aussi médiatisé et rassemblant des personnalités du monde entier reste une cible de choix pour les terroristes.

4. IDENTIFICATION DES RISQUES MAJEURS

4.1. ACTIONS VISANT L'ORGANISATION DE L'ÉVÈNEMENT

STADES ET INFRASTRUCTURES SPORTIVES

La sécurité de toutes les grandes infrastructures de divertissement accueillant une foule nombreuse est un véritable challenge. Et au sommet de ces infrastructures se trouvent les stades. Ces installations, dans lesquelles des dizaines de milliers de personnes se retrouvent au même moment, sont de plus en plus automatisées, connectées et gérées par des systèmes informatiques complexes de type « *Building Management Systems* ». Ascenseurs, climatisation, systèmes de sécurité physique, systèmes de vidéo et audio diffusion, systèmes d'aide à l'arbitrage, Wifi public… Comme l'ensemble des équipements numériques, tous ces systèmes présentent des failles de sécurité pouvant conduire à des cyber-attaques. Les systèmes dits « industriels » ne sont pas épargnés, loin de là, et vont même très certainement devenir la cible prioritaire d'attaques d'envergure dans le cadre de cyberguerre ou de cyber-terrorisme. Au point que certains experts du Center for Long-Term Cybersecurity de l'Université de Berkeley préconisent dans une étude récente une redondance avec des technologies analogiques pour les systèmes les plus sensibles[1].

SCENARIOS POSSIBLES

• Sabotage de l'air conditionné, particulièrement impactant pour des compétitions se déroulant dans les pays chauds, comme la Coupe du Monde de Football au Qatar.

• Sabotage de l'infrastructure électrique du stade.

• Prise de contrôle des systèmes d'affichage, pour la diffusion au moment opportun d'images de propagande.

• Blocage des ascenseurs d'accès aux gradins.

• Piratage général des systèmes des réseaux Wifi publics, avec vol de données sur les équipements mobiles compromis ou injection de malwares.

• Leurrage ou déni de service des équipements de mesure de la performance sportive ou des systèmes d'aide à l'arbitrage (ce point est particulièrement sensible pour les sports nécessitant une précision absolue, rendant illusoire toute intervention humaine : natation, course de vitesse…).

---

[1] *https://cltc.berkeley.edu/2017/10/10/cltc-issues-report-on-the-cybersecurity-of-olympic-sports/*

Article fictif : coupure électrique lors des JO 2024 à Paris

ACCUEIL DES SPORTIFS ET DES SUPPORTERS

Un grand événement sportif peut également être perturbé en dehors du stade. Les infrastructures d'accueil des délégations, officielles ou hôtelières, sont de plus en plus numérisées. A l'image du hacking du « Lakeside Alpine Hotel » en Autriche fin 2016, où une douzaine de clients se sont vus bloqués dans leurs chambres à cause d'un ransomware, la sécurité informatique de ces infrastructures laisse parfois à désirer, et passe trop souvent sous les radars des organisateurs. Imaginez toute une équipe bloquée dans son hôtel le matin même de la Finale d'une Coupe du Monde… Ce genre d'incident est monnaie courante, mais les hôtels ne souhaitent pas en parler pour ne pas inquiéter leurs clients. Que se passerait-il si, au lieu d'une demande de rançon, le système informatique avait définitivement bloqué les ouvertures des portes ?

De même, imaginez la nuit que passerait la même équipe si l'alarme incendie retentissait toutes les heures…

Enfin, les réfrigérateurs et les chambres froides, surtout dans les pays les plus chauds, sont indispensables pour la bonne conservation des aliments. Et ceux-ci sont de plus en plus dépendants de systèmes numérisés pour le contrôle précis de la température. Encore une fois, ces systèmes sont hautement vulnérables.

Une cyber-attaque peut se nicher derrière tout équipement numérisé, même le plus anodin, même non connecté à Internet. Les cibles les plus critiques ne sont parfois pas celles auxquelles on pense immédiatement, d'autant que les moyens techniques nécessaires ne sont pas d'une complexité extrême au vu du peu de protection de certains systèmes.

SCENARIOS POSSIBLES

• Sabotage des transports (métro, trains, signaux de trafic routier, aéroports). Ces systèmes sont généralement bien protégés, mais une attaque avancée peut néanmoins être conduite par des organisations bien structurées, étatiques ou paraétatiques. L'un des incidents les plus marquants s'est produit en juin 2015, lorsque la compagnie aérienne nationale polonaise LOT a annoncé l'annulation de 20 vols suite à une cyberattaque contre l'aéroport à Varsovie. A l'avenir les futurs systèmes de navettes autonomes acheminant les spectateurs peuvent aussi être visés.

• Sabotage de la qualité de l'eau courante.

• Sabotage de la génération ou de la distribution électrique.

• Sabotage des climatisations automatiques.

• Attaques informatiques sur les infrastructures médicales.

ACTIONS DANS LE CYBERESPACE EN SOUTIEN D'UN ACTE TERRORISTE

• Induction de panique dans le stade (alerte à la bombe ou message d'évacuation générale, mouvement de panique puis attentat-suicide ou bombe à la sortie du stade, avant les détecteurs).

• Hacking des systèmes de vidéo-surveillance, de détection de métaux / explosifs pour faciliter l'entrée de terroristes armés.

La plupart des systèmes de caméras de vidéosurveillance utilisent un noyau logiciel standard (généralement Windows) particulièrement sensible aux attaques informatiques. Leur sécurité n'a pas été pensée dès la conception, ou trop peu. Fort heureusement, certains constructeurs en font un critère différenciant, à l'image de Mobotix et son concept de cybersécurité « Cactus », ou de Honeywell qui intègre dans toutes ses caméras des puces qui contiennent une clé d'identification unique chiffrée. Mais le hacking de centaines de caméras de surveillance durant la cérémonie d'investiture de Donald Trump nous montre qu'aucun système n'est infaillible…

Article fictif : fausse alerte à la bombe au Stade de France en 2023

4.2. ACTIONS VISANT LES DÉLÉGATIONS ET LES SPORTIFS

Les sportifs eux-mêmes peuvent être la cible d'attaques, dans le but de les dénigrer ou de voler des données sur leurs stratégie de jeu, voire de falsifier leurs performances. Nous avons vu précédemment l'exemple du groupe de hackers russes Fancy Bear qui publie régulièrement des données médicales relatives aux sportifs pour dénoncer des cas supposés ou avérés de dopage. Plus subtilement, au lieu d'être simplement volées et mises sur la place publique, des données médicales pourraient aussi être falsifiées pour faire apparaître des cas de dopage qui n'en sont pas et discréditer un sportif pendant une compétition.

L'arrivée future de nouveaux systèmes électroniques et d'intelligence artificielle permettant de juger la performance d'un athlète n'est pas sans risques. Hauteur d'un saut à ski, attitude physique d'un gymnaste, hors-jeux, temps au centième de seconde lors d'une course de natation… Ces systèmes apportent précision et rapidité d'analyse. Mais imaginez maintenant que ces systèmes fournissent systématiquement des informations erronées mais crédibles, favorisant un athlète ou un pays dans sa course aux médailles… et que ces erreurs soient le fait d'un piratage informatique… Chaque nouvelle opportunité s'accompagne de nouveaux risques.

Des campagnes massives de dénigrement de sportifs ou d'équipes peuvent être orchestrées pour porter atteinte à leur moral : diffusion de données personnelles (photos ou vidéo compromettantes, comptes en banque, contenus de boites mails…), *fake news*… Ceci peut s'orchestrer en amont ou pendant la compétition, dans la relative impunité offerte par les techniques d'anonymisation sur le Net (VPN, paiement de ressources serveur en bitcoin, utilisation de TOR...).

SCENARIOS POSSIBLES

• Vol et publication de données médicales d'athlètes.

• Falsification de données médicales, dont les tests anti-dopage.

• Compromission d'e-mails d'athlètes ou de membres de délégations.

• Vol des données préparatoires aux compétitions (stratégies et tactiques des équipes, schémas de préparation des sportifs…).

• Prise de contrôle de l'affichage des scores.

• Campagnes de dénigrement des sportifs, *fake news*.

4.3. ACTIONS VISANT LE BUSINESS DU SPORT

Les grandes compétitions sportives sont l'un des business les plus importants de la planète : sponsors, produits dérivés, droit de retransmission, salaire des joueurs, tickets d'accès aux stades, afflux de supporters prompts à la dépense… Au-delà du sport lui-même, la cybercriminalité va viser l'ensemble des flux financiers liés à l'événement. Les hacktivistes y verront également une occasion unique de toucher une large audience.

SCENARIOS POSSIBLES

• Attaque du réseau de retransmission (Broadcasting) de la compétition. L'exemple de TV5 Monde est frappant. Un tel scénario, rendant impossible toute télédiffusion des compétitions pendant des jours, est tout à fait réaliste.

• Propagation de malwares via les nombreux sites pirates de retransmission des compétitions.

• Achat massif de tickets via des réseaux de botnets, puis revente au marché noir. Tous les outils sont librement téléchargeables, et accessible aux non-initiés. De plus, certains sites, dont le fameux ticketbots.net, rendent ce service accessible à tous. Ce site propose par ailleurs un outil de copie des codes-barres uniques de vrais billets, afin de réaliser de faux billets parfaitement réalistes.

• Multiplication de sites vendant de faux tickets.

• Attaques en déni de service sur les sites officiels de la compétition, pour perturber l'achat des billets.

• Piégeage des terminaux de paiement et distributeurs automatiques aux abords des stades pour voler des données bancaires.

• Campagne de dénigrement de sponsors.

• Attaque en déni de service sur les sites de paris en ligne, pour demande de rançons.

• Déni de service sur les sites utilisés par les agences de presse.

4.4. ACTIONS VISANT LES SYSTÈMES DE L'ETAT HÔTE

Les gouvernements font face quotidiennement à des menaces cyber. Leurs sites Web sont la cible d'attaques DDoS, de défacements par des hacktivistes et de vol de données. Ces données (contenus de boites mails de responsables, données confidentielles diverses) sont ensuite divulguées au public ou exploitées à des fins de renseignement.

L'organisation des grands événements sportifs dépend fortement du soutien des services gouvernementaux. C'est le gouvernement du pays hôte qui assure l'arrivée et l'accès des visiteurs, la sécurité et la légalité de l'événement, la communication et le transport, l'accès à l'information et d'autres tâches administratives. Par exemple, avec l'afflux de visiteurs entrant dans le pays, les services consulaires devront être rapides et efficaces dans la délivrance des visas. Les systèmes nécessaires pour enregistrer les informations requises et traiter l'émission des visas devront être protégés contre les acteurs malveillants cherchant à interrompre le service, à voler l'information ou à faire des bénéfices grâce à de l'intermédiation de services. Il existe ainsi plusieurs sites non officiels permettant de demander un ESTA (Electronic System for Travel Authorization) pour l'entrée aux Etats-Unis. Ces sites facturent entre 60 et 80 dollars US, alors que le site officiel, tout aussi ergonomique, n'en demande que 14…

SCENARIOS POSSIBLES

• Arnaque à la délivrance de visa visant les visiteurs de certains pays, ou perturbation du système par DDoS.

• Défacement ou DDoS de sites gouvernementaux liés à l'événement.

• Vol de données de membres du gouvernement du pays hôte (comptes mails, données sensibles…).

Ce type de scénario démontre la façon dont même une attaque simple est susceptible de provoquer des conséquences directes sur les objectifs que le pays hôte espère atteindre grâce à l'organisation d'un grand évènement sportif. L'opinion publique internationale pourrait considérer que les services publics et les infrastructures du pays hôte ne sont pas à la hauteur de l'événement, jetant le discrédit sur le pays tout entier.

5. TABLEAU DE SYNTHÈSE

Le tableau de synthèse suivant regroupe l'ensemble des risques identifiés dans cette note (sans bien sûr prétendre à l'exhaustivité), en indiquant trois variables permettant de les prioriser[2] :

• Son **impact**, i.e. sa capacité à compromettre la compétition ou à impacter sévèrement l'image de l'événement – note de 1 (impact faible, la compétition continue sans gêne apparente), à 5 (impact maximal, la compétition est définitivement arrêtée)

• sa **probabilité d'occurrence**, calculée en fonction des motivations, de la complexité de réalisation de l'attaque, des moyens nécessaires et des capacités actuelles des équipements de sécurité numérique potentiellement mis en place ou de l'existence de plans de secours – note de 1 (probabilité faible) à 5 (probabilité très forte)

• sa **détectabilit**é : capacité de détection de la menace en amont de son effet – note de 1 (attaque facilement détectable) à 5 (attaque très furtive)

ORGANISATION DE L'ÉVÉNEMENT

STADES ET INFRASTRUCTURES SPORTIVES

Risque	Impact	Proba.	Detect.
Sabotage de l'air conditionné des stades	3	2	4
Sabotage de l'infrastructure électrique	5	2	4
Prise de contrôle des systèmes d'affichage	2	3	4
Blocage des ascenseurs	2	2	5
Piratage du Wifi public – vol de données	1	4	1
Piratage des systèmes de mesure de la performance sportive	5	3	4

[2] *Ces données n'engagent que les auteurs. Elles doivent être consolidées par une analyse de risque exhaustive.*

ACCUEIL DES SPORTIFS ET DES SUPPORTERS

Risque	Impact	Proba.	Detect.
Sabotage des transports	2 à 5	2	2
Eau courante	2	2	2
Réseau électrique général	5	2	2
Climatisations (hors stade)	2	2	5
Infrastructures médicales	2	2	4

ACTIONS DANS LE CYBERESPACE EN SOUTIEN D'UN ACTE TERRORISTE

Risque	Impact	Proba.	Detect.
Induction de panique dans le stade	5	2	4
Hacking des systèmes de sécurité physique pour faciliter un acte terroriste	5	2	4

ACTIONS VISANT LES DÉLÉGATIONS ET LES SPORTIFS

Risque	Impact	Proba.	Detect.
Vol de données médicales d'athlètes	2	5	3
Falsification de données médicales (contrôle anti-dopage)	3	3	5
Compromission de boites mails	1	5	4
Vol de données préparatoires aux compétitions	3	3	5
Prise de contrôle de l'affichage des scores	3	2	4
Campagnes de dénigrement	1	5	5

ACTIONS VISANT LES DÉLÉGATIONS ET LES SPORTIFS

Risque	Impact	Proba.	Detect.
Attaque du réseau de retransmission TV des compétitions	5	3	4
Propagation de malwares via des sites de retransmission pirates	1	5	2
Achats massifs de tickets via des botnets	2	5	2
Vente massive de faux billets	3	4	2
DDoS sur les sites commerciaux officiels	2	5	3
Piège des terminaux de paiement et/ou distributeurs de billets	1	4	3
Dénigrement des sponsors	1	5	5
DDoS sur les sites de paris en ligne	1	4	3
DDoS sur les sites des agences de presse	2	4	3

ACTIONS DANS LE CYBERESPACE EN SOUTIEN D'UN ACTE TERRORISTE

Risque	Impact	Proba.	Detect.
Arnaque à la délivrance de visas ou DDoS	3	3	2
Défacement ou DDoS sur les sites gouvernementaux	1	4	2
Vol de données de personnalités du gouvernement hôte	1	5	4

6. RECOMMANDATIONS

En amont des compétitions, bien se préparer au risque est indispensable. Les spécifications des équipements utilisés doivent absolument intégrer la cybersécurité « by design », et de nombreux tests de vulnérabilité doivent être conduits avant toute mise en production ou acceptation par les décideurs.

Cette méthodologie ne pourra être mise en place que si la prise de conscience du risque est effective. Il conviendra donc, très en amont de l'événement, de mettre en place une cellule d'analyse et d'investigation sur les risques potentiels ou avérés, d'abord au niveau stratégique, puis, la compétition approchant, au niveau opérationnel.

Cette cellule élaborera des scénarios d'attaques sur tous les domaines identifiés, et les personnels en charge de la sécurité informatique s'entraîneront à faire face à un grand nombre d'attaques dans un *Cyber Training Center* tel que celui de bluecyforce en France, capable de reproduire à des fins de formation et d'entraînement à la crise des schémas d'attaques réalistes.

Tous les acteurs doivent être impliqués, pas uniquement ceux prenant directement part à l'organisation. Cela impose la mise en place d'une politique nationale de cybersécurité efficace, en coordination avec les nations participantes et les organismes internationaux en charge de la sécurité.

Une fois les systèmes critiques identifiés, il convient de mettre en place très en amont de l'événement une unité de *Cyber Threat Intelligence* capable d'identifier en temps-réel toute les vulnérabilités externes (fuites de données, vente de malwares ciblés dans le Dark Web, sites frauduleux, *typosquatting*, suivi des média sociaux, vulnérabilités des sites Web, suivi des hacktivistes, données volées accessibles sur le Deep et le Dark Web…).

En interne, un ou plusieurs *Security Operational Center* seront mis en place, coordonnant l'ensemble des actions de sécurité numérique.

Pendant la compétition, une équipe de « pompiers du numérique » suffisamment bien dimensionnée (CERT, CSIRT), sera à disposition de toutes les entités concernées, 24h sur 24. Au besoin, l'Etat hôte pourra faire appel à une structure de réservistes opérationnels pour faire face à une attaque de grande ampleur.

En cas d'attaque bloquante, un PRA/PCA (plan de continuité et de reprise d'activité), aura été mis en place et testé au réel lors d'exercices de crise grandeur réelle effectués en amont.

Les acteurs étant très nombreux, il conviendra de monter un centre dédié au partage des informations de sécurité, à l'image de l'ISAO (*Information Sharing and Analysis Organization*) aux Etats-Unis qui surveille, analyse et répond aux risques cyber spécifiquement liés au sport.

Après l'événement, le partage d'information doit continuer entre les Etats et les organisations sportives, qui doivent améliorer leur coopération sur le sujet (CIO, FIFA, Rugby League, UEFA, Ligues Américaines, CAN…), afin que les pays hôtes suivant puissent améliorer sa préparation.

Les enjeux financiers et humains sont tels que les diverses organisations doivent mieux coopérer et allier leurs efforts, pour que les grands évènements sportifs puissent rester les succès populaires qu'ils sont aujourd'hui.

PUBLICATIONS RÉCENTES

Le Plan d'action de la Commission européenne pour la Défense – une initiative encourageante mais à l'avenir encore incertain (Septembre 2017)

La survivabilité des hélicoptères : une préoccupation au coeur des engagements modernes, un enjeu majeur pour demain (Septembre 2017)

Le Système d'information des Armées (SIA) – Le programme SIA : changement de paradigme pour l'armée du futur (Août 2017)

Internet des Objets (IoT)- Une nouvelle donne pour la Défense ? (Août 2017)

Impression 3D – Des technologies de rupture au service des Armées (Août 2017)

Emploi du Cloud dans les armées – Première approche des concepts et contraintes (Août 2017)

Enjeux stratégiques du Big Data pour la Défense (Août 2017)

Cybersécurité dans le milieu maritime (Février 2017)

Android Malware in 2016: the emergence of a professional ecosystem (Janvier 2017)

A télécharger sur **www.sia-lab.fr** et **www.ceis.eu**

Compagnie Européenne d'Intelligence Stratégique (CEIS)

Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 00022 – APE : 741 G

280 boulevard Saint Germain – 75007 Paris

Tél. : **01 45 55 00 20** – Fax : **01 45 55 00 60**

Tous droits réservés