GEMA..

GRANDES ECOLES DES MÉTIERS D'AVENIR

Projet Cyber

en vue de l'obtention du diplôme de

Bachelor 3 en Cybersécurité & Buisness

par

Akazaf Abdellah

Jeux Olympiques 2024 : Identifier et prévenir les risques cyber

PARIS 2024

CYBER Management School

Encadré par l'équipe pédagogique

Sommaire

CYBER Management School

I. Résumé

Les Jeux Olympiques de Paris 2024 représentent un événement d'envergure mondiale, avec un budget de 9 milliards d'euros et des recettes prévues à 1,2 milliard d'euros. Cet événement rassemblera plus de 16 millions de personnes, incluant spectateurs, touristes, athlètes et délégations politiques. Cependant, les Jeux Olympiques constituent une cible de choix pour les cybercriminels, qui pourraient mener des attaques par appât du gain, par volonté de nuire ou dans un but d'espionnage. Depuis les Jeux de Londres en 2012, on constate une forte augmentation de l'activité cybercriminelle, avec jusqu'à 450 millions d'attaques recensées lors des Jeux de Tokyo en 2018.

Ce projet de remédiation vise à identifier les principaux actifs à protéger, analyser quatre scénarios de risques réalistes et de proposer des mesures concrètes pour réduire ces risques et garantir la sécurité de l'événement. Les mesures proposées couvrent différents aspects de la cybersécurité, allant du renforcement des contrôles techniques à la mise en place de procédures organisationnelles et de plans de gestion de crise.

En conclusion, ce projet offre une analyse approfondie des risques cyber et des solutions pratiques pour assurer la sécurité des Jeux Olympiques de Paris 2024, permettant ainsi de minimiser les risques et de garantir le bon déroulement de cet événement international majeur.

II. Introduction

Les Jeux Olympiques de Paris 2024 présentent des défis considérables en matière de logistique, de sécurité et de technologie. Cet événement, qui attire plusieurs millions de spectateurs, athlètes et délégations du monde entier, repose sur des infrastructures numériques complexes pour la gestion des compétitions, la diffusion des événements, la billetterie et les communications. La cybersécurité est absolument cruciale pour prévenir les incidents susceptibles de perturber les Jeux, de compromettre les données ou de nuire à la réputation de l'événement ou du pays.

Avec un budget important et une audience mondiale, les Jeux Olympiques sont alors une cible privilégiée pour les cybercriminels, motivés par des gains financiers énormes, la volonté de nuire ou des objectifs d'espionnage. Depuis les Jeux

Olympiques de Londres en 2012, les cyberattaques associées à ces événements ont considérablement augmenté, atteignant 450 millions d'attaques lors des Jeux de Tokyo en 2018. La France doit donc se préparer à contrer ces menaces qui vont augmenter avec l'ascension du numérique ces dernières années pour assurer un déroulement sans perturbation des Jeux.

Ce projet de remédiation se concentre sur l'identification des actifs pour assurer un bon déroulement des Jeux Olympiques, l'analyse de quatre scénarios de risques réalistes sur ces actifs et la proposition de mesures concrètes de remédiation pour atténuer ces risques.

Le projet est structuré de la manière suivante :

- Identification des actifs : Déterminer les actifs et les données critiques nécessitant une protection renforcée ainsi que leurs besoins de sécurité.

- Scénario de risques et impacts : Analyser les attaques potentielles sur ces actifs, leur niveau de risque et leurs conséquences.

- Remédiation : Proposer des mesures pour réduire leur niveau de risque et atténuer la probabilité d'occurrence de ces scénarios.

- Conclusion : Synthétiser les recommandations et les perspectives pour garantir la cybersécurité des Jeux Olympiques de Paris 2024.

Cette structure vise à offrir une analyse approfondie des risques cyber et à proposer des solutions pratiques pour assurer la sécurité de cet événement international majeur.

III. Identification des actifs

Les principaux actifs identifiés à protéger dans le cadre des Jeux Olympiques de Paris 2024 sont :

- **Systèmes de gestion des compétitions**

Ces systèmes comprennent le chronométrage, la gestion des résultats et la diffusion des informations aux spectateurs et aux médias.

- Disponibilité : Les systèmes doivent être opérationnels en permanence pour assurer le bon déroulement des compétitions sans interruption.

- Intégrité : Les résultats et les données de chronométrage doivent être exacts pour garantir l'égalité des compétiteurs.

- Confidentialité : Les informations sensibles, telles que les stratégies des équipes et les données non encore publiées, doivent être protégées contre des accès non autorisés.

- **Plateformes de diffusion des événements**

Le site web officiel des Jeux, les différentes applications mobiles et les réseaux sociaux permettent de diffuser en direct les événements sportifs et de communiquer avec le public.

- Disponibilité : Les plateformes doivent être accessibles en permanence pour permettre une diffusion sans interruption des événements en direct.

- Intégrité : Le contenu diffusé doit être authentique et protéger contre des modifications non autorisées ou malveillantes qui pourraient changer le sens ou la nature des informations.

- Confidentialité : Les données utilisateur et les informations de compte doivent être protégées contre les accès non autorisés et les violations de données.

- **Systèmes de billetterie et de contrôle d'accès**

Ces systèmes gèrent la vente des billets et le contrôle d'accès sur les sites des compétitions.

- Disponibilité : Les systèmes de billetterie et de contrôle d'accès doivent fonctionner sans interruption pour gérer efficacement les entrées des spectateurs.

- Intégrité : Les transactions et les billets doivent être exacts pour prévenir la fraude et les accès non autorisés.

- Confidentialité : Les informations personnelles des acheteurs de billets doivent être protégées contre les accès non autorisés et les vols de données.

- **Infrastructures de communication**

Les réseaux de télécommunication, les centres de données et les systèmes de sécurité physique permettent d'assurer la connectivité et la sécurité de l'événement.

- Disponibilité : Les infrastructures de communication doivent être opérationnelles en permanence pour assurer une connectivité continue.

- Intégrité : Les données transmises via les réseaux doivent être protégées contre toute interception non autorisée.

- Confidentialité : Les communications, particulièrement celles contenant des informations sensibles, doivent être protégées contre les écoutes et les intrusions.

- **Données personnelles des athlètes, du personnel et des spectateurs**

Ces données, qui incluent des informations médicales, d'accréditation et de billetterie, doivent être protégées contre tout accès non autorisé afin de préserver la vie privée des personnes.

- Disponibilité : Les données doivent être accessibles aux personnes autorisées en continue pour une gestion efficace des compétitions et des services.

- Intégrité : Les informations doivent être exactes et ne doivent pas être modifiées de manière non autorisée.

- Confidentialité : Les données personnelles doivent être strictement protégées contre les accès non autorisés et les violations de confidentialité.

Ces actifs ont des besoins spécifiques en termes de disponibilité, d'intégrité et de confidentialité, qui doivent être pris en compte dans la définition des mesures de sécurité.

IV. Scénario de risques et impacts

Scénario 1 : Attaque de désinformation sur les réseaux sociaux

Pour mettre en place une attaque de désinformation, un groupe de propagandistes lance une campagne de désinformation coordonnée sur les réseaux sociaux, visant

à ternir l'image et la crédibilité des Jeux Olympiques. Pour se faire ils utilisent un grand nombre de faux comptes sur les réseaux sociaux, ils diffusent de fausses informations et ils ciblent des audiences vulnérables.

Le niveau de risque est moyen. Avec la facilité pour créer et gérer des faux comptes et des événements internationaux ont déjà été ciblés par des campagnes de désinformation, montrant que cette tactique est couramment utilisée.

Les impacts potentiels sont la perte de confiance du public, l'impact négatif sur l'image de marque de l'événement, les risques de perturbations logistiques. Ce scénario est déjà survenu lors des Jeux Olympiques de Rio en 2016, des fausses informations sur le virus Zika avaient circulé sur les réseaux sociaux, entraînant des inquiétudes et une baisse de la fréquentation.

Scénario 2 : Compromission des systèmes de billetterie

Pour compromettre les systèmes de billetterie des Jeux Olympiques, les attaquants pourraient envoyer des emails de phishing ciblés aux employés ayant accès aux systèmes de billetterie. Une fois à l'intérieur du système, les attaquants cherchent à escalader leurs privilèges pour obtenir un accès administratif complet. Avec un accès administratif, les attaquants peuvent modifier les données de billetterie, créer des billets frauduleux, annuler des billets valides ou accéder à des informations personnelles des détenteurs de billets.

Le niveau de risque est moyen à élevé. Les systèmes de billetterie en ligne sont des cibles fréquentes pour les cybercriminels, en raison de la valeur des informations qu'ils contiennent. Les méthodes d'attaque sont aussi très variées, allant du phishing à l'exploitation de vulnérabilités, ce qui augmente la probabilité de succès.

Les impacts potentiels sont l'affluence incontrôlée sur le site, risques de sécurité physique, perte de revenus pour l'organisation, atteinte à l'image de l'événement. Ce scénario fait écho aux incidents survenus lors des Jeux Olympiques de Londres en 2012, où des pirates informatiques avaient réussi à s'introduire dans les systèmes de billetterie, entraînant un afflux massif de spectateurs non autorisés.

Scénario 3 : Fuite de données personnelles des participants

Pour réaliser une fuite de données personnelles des participants des Jeux Olympiques, les possibilités sont nombreuses. Les attaquants envoient des emails de phishing sophistiqués aux employés ou aux fournisseurs de services ayant accès aux bases de données des participants. Une attaque interne où un employé mal

intentionné subtilise les données personnelles d'athlètes et de spectateurs, et les revend sur le darknet.

Le niveau de risque est élevé. En effet, les multiples points d'entrée (employés, fournisseurs, partenaires) et les divers systèmes interconnectés augmentent les opportunités pour les attaquants d'exploiter des failles de sécurité.

Les impacts potentiels sont l'atteinte à la vie privée des victimes, les risques de chantage et l'impact médiatique négatif pour l'organisation.

Scénario 4 : Attaque par déni de service contre les systèmes de gestion des compétitions

L'objectif de cette attaque est de rendre les systèmes de gestion des compétitions indisponibles, perturbant ainsi le chronométrage, la gestion des résultats et la diffusion des informations, ce qui entraîne des interruptions et un chaos organisationnel pendant les compétitions. Les attaquants mènent une reconnaissance sur les infrastructures des Jeux Olympiques pour identifier les points faibles et les serveurs critiques liés à la gestion des compétitions. Ils surveillent le trafic et cartographient des adresses IP pour repérer les moments vulnérables. Cette attaque vise à saturer les ressources du serveur.

Le niveau de risque est élevé pour ce scénario. En effet, les attaquants peuvent louer des botnets ou utiliser des logiciels malveillants pour lancer des attaques, ces outils sont facilement disponibles sur le dark net.

Les impacts potentiels sont l'interruption des compétitions, la frustration des spectateurs, la remise en cause de l'intégrité des résultats, l'impact médiatique négatif. Ce scénario n'est pas inédit, puisque lors des Jeux Olympiques de Pyeongchang en 2018, les systèmes de chronométrage et de diffusion des résultats ont été touchés par une attaque par déni de service, entraînant des retards et des perturbations pendant les épreuves.

Ces quatres scénarios potentiellement hypothétiques, s'appuient sur des exemples concrets d'incidents de cybersécurité survenus lors d'éditions précédentes des Jeux Olympiques. Ils illustrent la diversité et la gravité des menaces auxquelles les organisateurs de l'événement de Paris 2024 devront faire face.

V. Remédiation

Renforcement de la sécurité des systèmes informatiques

1. Contrôles d'accès renforcés

   - Implémentation d'une authentification multifactorielle et de chiffrement des données pour les systèmes critiques. Ces mesures visent à limiter les accès non autorisés et à protéger l'intégrité des données.

2. Détection et protection contre les attaques par déni de service

   - Mise en place de pare-feux et de systèmes de prévention d'intrusion. Ces solutions permettront de détecter et de bloquer rapidement les tentatives d'attaque, préservant ainsi la disponibilité des systèmes critiques.

3. Systèmes de sauvegarde et de récupération en cas de sinistre

   - Déploiement de solutions permettant de restaurer rapidement les services essentiels en cas d'incident. Cela assurera la continuité des opérations et préservera la disponibilité des systèmes.

Amélioration de la gestion des identités et des accès

1. Authentification multifactorielle

   - Mise en place pour l'accès aux systèmes sensibles, en s'appuyant sur des technologies biométriques par exemple. Cela renforcera la sécurité des accès et limitera les risques de compromission.

2. Sensibilisation du personnel

   - Formation aux bonnes pratiques de cybersécurité, notamment en matière de gestion des mots de passe et d'utilisation des réseaux sociaux. Cela réduira les risques liés aux erreurs humaines.

3. Politiques de gestion des habilitations

   - Définition de politiques strictes de gestion des droits d'accès, avec un suivi et un audit régulier. Cela permettra de s'assurer que seules les personnes

autorisées ont accès aux informations et aux systèmes critiques.

Préparer l'organisation face aux incidents

1. Plans de continuité d'activité et de gestion de crise

   - Élaboration de plans permettant de maintenir les opérations essentielles en cas d'incident. Cela assure la continuité de l'événement malgré l'apparition d'un incident de sécurité.

2. Exercices et simulations réguliers

   - Tests des procédures et de la capacité de réponse de l'organisation. Cela permettra d'identifier et de corriger les failles dans la préparation de l'événement.

3. Partenariats avec les autorités compétentes

   - Collaboration avec la police, la gendarmerie et l'ANSSI pour la gestion des incidents de sécurité. Cela facilitera la coordination et la réponse en cas d'événement majeur.

Surveillance et réponse face aux menaces

1. Centre opérationnel de sécurité (SOC)

   - Déploiement pour la détection et la réponse aux incidents, en s'appuyant sur des solutions de sécurité avancées. Cela permettra de surveiller en permanence les activités suspectes et de réagir rapidement en cas d'incident.

2. Veille stratégique sur les menaces émergentes

   - Collaboration avec des experts en cybersécurité pour anticiper les nouvelles menaces et adapter les mesures de sécurité en conséquence.

3. Coordination avec les équipes de communication

   - Gestion de l'impact médiatique des incidents pour limiter les dommages à l'image de l'événement en cas d'incident de sécurité.

Pour garantir la sécurité et la résilience des Jeux Olympiques de Paris 2024 face aux menaces cyber, une approche multi-facette est nécessaire. Ces mesures de remédiation couvrent différents aspects de la cybersécurité, allant du renforcement des contrôles techniques à la mise en place de procédures organisationnelles et de plans de gestion de crise. En combinant ces stratégies, les organisateurs peuvent minimiser les risques et garantir le bon déroulement de cet événement international majeur.

VI. Conclusion

Ce projet de remédiation a permis d'identifier les principaux actifs à protéger dans le cadre des Jeux Olympiques de Paris 2024 et d'analyser quatre scénarios de risques réalistes, s'appuyant sur des exemples concrets issus d'éditions précédentes. Les mesures de sécurité proposées couvrent différents aspects de la cybersécurité, allant du renforcement des contrôles techniques à la mise en place de procédures organisationnelles et de plans de gestion de crise. Leur mise en œuvre permettra de réduire de manière significative les risques pesant sur la sécurité et la réussite de cet événement international majeur.

Au-delà de l'organisation des Jeux Olympiques, ce projet de remédiation offre une vision des enjeux de cybersécurité auxquels les organisations de tous secteurs d'activité seront confrontées dans les années à venir. Il illustre l'importance de l'innovation et de la préparation face à des menaces cyber en constante évolution, afin de garantir la sécurité et la résilience de systèmes essentiels au bon fonctionnement de notre société.

Ce projet met en lumière les défis spécifiques de cybersécurité auxquels les organisateurs des Jeux Olympiques de Paris 2024 devront faire face. En s'appuyant sur des exemples concrets d'incidents survenus lors d'éditions précédentes, il permet d'identifier des scénarios de risques réalistes et de proposer des mesures de sécurité adaptées.

Annexe

Sources :

https://www.stormshield.com/fr/actus/cybersecurite-jeux-olympiques-retour-experience-avant-paris-2024/

https://incyber.org/article/cybersecurite-des-jo-de-paris-2024-un-defi-collectif/

https://www.portail-ie.fr/univers/risques-et-gouvernance-cyber/2024/cyberattaques-aux-jeux-olympiques-et-paralympiques-2024-enjeux-mythes-et-realite/#:~:text=Le%20nombre%20de%20cyberattaques%20lors,sont%20attendues%20en%20juillet%202024.

https://www.cci.fr/actualites/jop-paris-2024-et-si-les-hackers-entraient-en-jeu

https://www.lemondeinformatique.fr/les-dossiers/lire-jo-et-cyber-attaques-plus-haut-plus-loin-plus-fort-1507.html