cyber sécurité : Chaire grands évènements publics
Fondation Université Bretagne Sud

PARIS 2024 : CYBERSÉCURITÉ, QUEL BILAN ?

RAPPORT D'ÉVÉNEMENT

10 DÉCEMBRE 2024
MAISON DE LA BRETAGNE - PARIS

Fondation : Université Bretagne Sud

INTRODUCTION

Le mardi 10 décembre, la Chaire Cybersécurité des Grands Evénements Publics, portée par la Fondation Université Bretagne Sud, a organisé une rencontre autour de la cybersécurité des Jeux Olympiques 2024.

L'événement s'est déroulé à la Maison de la Bretagne à Paris où sont intervenus des acteurs de premier plan qui ont assuré la cybersécurité de l'événement : les industriels, la gendarmerie, le ComCyber MI.

BILAN GÉNÉRAL ET TECHNIQUE

Cybersécurité Paris 2024, un défi réussi ?

Les Jeux Olympiques et Paralympiques de Paris 2024 étaient un événement sans précédent, à la fois par leur ampleur et les défis numériques à relever. **Plus de 10 000 athlètes, plus de 100 000 emplois, plus de 500 sites à surveiller (dont 95% dans des lieux patrimoniaux), des milliards de spectateurs à travers le monde et un environnement hyperconnecté.** Ainsi, la sécurité des infrastructures numériques et la protection contre les cybermenaces sont devenues des priorités absolues. Plus de 4 milliards de cyberattaques avaient été annoncées.
Selon l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), 548 cyberattaques majeures ont été recensées pendant la période des Jeux. Pas de sensationnalisme. En vérité il y a bien eu 55 milliards « d'évènements ». Des nuances ont été apportées lors de ce retour d'expérience à travers des interventions complémentaires, pour comprendre :

- Les enjeux stratégiques et techniques de la cybersécurité lors des JO Paris 2024.
- Les enseignements concrets à retenir pour anticiper et protéger les grands événements futurs.
- La synergie réussie entre acteurs publics, industriels et institutions pour relever ce défi majeur.

1/ Enjeux, stratégies mises en place et résultats obtenus : une vision globale sur la cybersécurité des JO

Préambule de Gérard LACROIX, délégué général adjoint à la sécurité du GICAT (Groupement des Industries Françaises de Défense et de Sécurité terrestres et aéroterrestres) qui regroupe 460 entreprises membres dont Thales, Airbus, Atos ou Orange, qui jouent un rôle crucial dans la lutte contre la cybercriminalité en fournissant les moyens nécessaires à l'État pour contrer notamment les ingérences étrangères.

Cybersécurité Paris 2024, un défi réussi ?

Intervention de Yannick RAGONNEAU, directeur général du Programme Général de Sécurité (PGS) chez Eviden, en lien avec le Ministère de l'intérieur et la DGSN.

Son intervention a posé un propos général sur la technologie et l'innovation au service de l'engagement du public avant, pendant et après un événement.

- Avant l'événement : avec les expériences en réalité augmentée, le contenu gamifié et les recommandations personnalisées pour susciter de l'enthousiasme et de l'anticipation.
- Pendant l'événement : avec les écrans interactifs, l'intégration des réseaux sociaux et les mises à jour en temps réel pour créer une expérience immersive et engageante.
- Après l'événement : avec le contenu personnalisé, les sondages auprès du public et l'accès à des images exclusives des coulisses pour prolonger l'engagement au-delà de l'événement.

Il a insisté sur l'importance de l'intersection de la technologie et du sport qui évolue rapidement, transformant l'expérience pour les athlètes comme pour les spectateurs. L'amélioration des performances et l'optimisation de la sécurité démontrent que la technologie joue un rôle central dans les événements sportifs modernes à plusieurs niveaux. L'analyse de données aide les organisateurs à comprendre le comportement du public, à optimiser les prix et à personnaliser les expériences. Les plateformes cloud simplifient la communication, l'allocation des ressources et la collaboration entre les parties prenantes de l'événement et la cybersécurité pour protéger les données sensibles et assurer l'intégrité des systèmes est primordial pour la sécurité des événements.

Cybersécurité Paris 2024, un défi réussi ?

Il faut pouvoir contrôler l'ensemble de la chaîne de sécurité pour garantir une sécurité de bout en bout lors des grands événements, grâce à l'expertise, la capacité et l'expérience. Les Jeux Olympiques ont été un succès, accéléré par le dispositif de sécurité de grande envergure déployé dans un modèle de collaboration inédit. Les industriels de la sécurité ont su se positionner et apporter leur expertise et leurs technologies pour répondre aux quatre objectifs principaux :

- Garantir la sécurité et l'esprit festif des Jeux
- Améliorer considérablement les capacités des forces de sécurité interne
- Fédérer l'industrie de la sécurité française et en faire un champion international
- Contribuer à l'héritage du programme olympique

Grâce à la fédération de l'ensemble de l'industrie et à la direction et alignement DIJOP, SGDSN, ANSSI et ministère de l'Intérieur/DEPSA, le programme d'expérimentation a été l'un des piliers de cette initiative publique et privée originale et innovante. Le programme a été et est encore un véritable succès, grâce à sa nature innovante, la collaboration entre les forces de sécurité intérieure et les entreprises de toute taille. Les plus de 200 expérimentations ont déjà permis d'identifier les domaines clés nécessaires pour transformer le Ministère et l'industrie (technologie, gestion budgétaire / ROI, cadre juridique) tout en permettant d'intégrer une dimension d'héritage. Il s'agit de renforcer le partenariat et la collaboration public-privé car la sécurité et la sûreté relèvent de la notion de citoyenneté.

Paris 2024 a été un succès grâce à une préparation olympique et une approche « start-up », intégrant les bonnes pratiques de design thinking, open innovation, red teaming, collaboration, anti-Fragile, sensibilisation à la situation...
Yannick Ragonneau conclut que l'héritage de cette expérimentation permettra de :

- Établir des relations permanentes et stables (réserve, think tank, ...)
- Mettre en œuvre un laboratoire permanent d'expérimentations
- Développer une doctrine commune / des modèles opérationnels, des exercices, des tests
- Porter la collaboration à l'international via une équipe de France de la sécurité
- Intégrer l'ensemble des dimensions

Cybersécurité Paris 2024, un défi réussi ?

2/ La vision technique des systèmes de protection numérique déployés, des innovations majeures et des incidents gérés avec succès.

Intervention de Benoît DELPIERRE – Directeur en charge du projet Paris 2024 chez Eviden

Eviden, est une filiale d'Atos spécialisée dans le numérique sécurisé et la cybersécurité. Forte d'une expertise reconnue dans la gestion des systèmes critiques pour des événements internationaux, elle a piloté la mise en œuvre des infrastructures numériques essentielles pour assurer la sécurité technique des Jeux Olympiques de Paris 2024.

À la tête des équipes d'Eviden, Benoît Delpierre a supervisé la préparation et l'anticipation des menaces cybernétiques, garantissant la résilience des systèmes face aux attaques. Son bilan technique repose sur une détection proactive des menaces, des simulations rigoureuses et une collaboration étroite avec les acteurs publics et privés pour neutraliser plus de 850 incidentscyber, notamment les attaques par déni de service (DDoS), sans impact opérationnel.

Parmi ces incidents, les attaques par déni de service distribué (DDoS) ont été prédominantes, notamment lors de moments clés tels que la cérémonie d'ouverture et la finale du 100 mètres en athlétisme. Grâce à une préparation minutieuse, incluant des semaines de tests et de simulations, les équipes d'Eviden ont pu anticiper et neutraliser ces menaces sans perturber les systèmes en place.

Cybersécurité Paris 2024, un défi réussi ?

Cette réussite est attribuée à une stratégie d'anticipation rigoureuse et à une collaboration étroite entre les experts en cybersécurité et les autres métiers impliqués dans l'événementiel. Benoît Delpierre a également mis en avant l'importance de la détection proactive des signaux faibles, permettant d'identifier et de contrer les attaques avant qu'elles ne causent des dommages.

Son retour d'expérience met en lumière les innovations technologiques déployées, les enseignements tirés en matière de cybersécurité et la capacité des solutions françaises à s'imposer comme des références pour les futurs événements internationaux.

En conclusion, la gestion de la cybersécurité lors des JO de Paris 2024 a été saluée comme un succès, démontrant l'efficacité d'une préparation approfondie et d'une collaboration interdisciplinaire face aux menaces cybernétiques.

Cybersécurité Paris 2024, les leçons à retenir

Lors de la table ronde centrale de cette journée, quatre intervenants ont partagé leurs retours d'expérience : Daniel Le Coguic, vice-président d'Eviden ; Yannick Ragonneau, directeur du Programme Général de Sécurité (PGS) chez Eviden ; le Lieutenant-colonel Sophie Lambert, responsable au sein du Commandement du ministère de l'Intérieur dans le cyberespace ; et Madame la députée Anne Le Henanff, membre de la Commission de la défense nationale et rapporteure sur la transformation cyber du ministère des Armées. Ensemble, ils ont dressé un bilan technique, stratégique et humain de cet événement mondial.

Le succès de Paris 2024 a donc reposé sur une mobilisation exceptionnelle des acteurs publics et privés et des entités étatiques comme le ministère de l'Intérieur. La thématique de cette table a permis d'évaluer et de pointer les leçons tirées de cette expérience inédite avec les 4 intervenants présents, à l'horizon de futures échéances internationales et avec l'objectif de renforcer la résilience des infrastructures françaises face aux menaces cybernétiques lors de manifestations d'envergure mondiale. La question centrale était de comprendre l'héritage laissé par l'expérience Paris 2024.

Cybersécurité Paris 2024, les leçons à retenir

- Une coordination exemplaire et une anticipation rigoureuse

Dès l'ouverture, Daniel Le Coguic a mis en avant le caractère unique de Paris 2024, qualifié comme « les Jeux les plus numériques et sécurisés de l'histoire ». Selon lui, le succès repose sur une anticipation rigoureuse et une mobilisation sans précédent entre acteurs publics et privés. Avec l'appui de technologies de pointe développées par Eviden. Si des incidents de cybersécurité ont été répertoriés durant l'événement, aucun n'a perturbé le bon déroulement des compétitions.

De son côté, Yannick Ragonneau a partagé les détails techniques des solutions mises en place. Parmi les menaces les plus fréquentes figuraient les attaques par DDoS, notamment lors de moments sensibles comme la cérémonie d'ouverture. « Les simulations réalisées en amont nous ont permis d'être prêts. Chaque scénario a été testé pour garantir la résilience des infrastructures critiques », a-t-il expliqué.

- Collaboration public-privé et mobilisation humaine

Le Lieutenant-colonel Sophie Lambert a souligné la collaboration stratégique entre ministères, ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) et partenaires privés. Elle a également mis en avant le rôle crucial des réservistes, présents en soutien au Centre de coordination stratégique à Beauvau. « La préparation humaine a été aussi déterminante que les innovations technologiques. Nous avons appris à capitaliser sur des talents venus d'horizons divers », a-t-elle déclaré.

L'importance de la transparence et de la communication interservices a également été mise en lumière : « Pour contrer les menaces efficacement, il fallait partager les informations en temps réel sans rétention. Cette synergie a été la clé du succès », a affirmé Sophie Lambert.

- Une vision institutionnelle et des perspectives d'avenir

Madame la députée Anne Le Henanff a apporté un éclairage institutionnel, insistant sur l'importance de renforcer la souveraineté numérique de la France. « Paris 2024 a été un laboratoire pour les futures grandes échéances. Les enseignements tirés de cette expérience doivent nous permettre de préparer des événements encore plus complexes, tout en stimulant l'innovation technologique française », a-t-elle affirmé. Elle a également évoqué les perspectives d'exportation des solutions françaises vers des événements internationaux, tels que les Jeux de Los Angeles 2028.

CONCLUSION

Bilan : un modèle de référence

En conclusion, les intervenants se sont accordés à dire que les Jeux Olympiques de Paris 2024 ont été une réussite en termes de cybersécurité. L'anticipation, la collaboration public-privé et l'engagement humain ont permis de relever ce défi monumental. Les enseignements tirés de cette expérience serviront de modèle pour renforcer la sécurité des grands événements à venir.

Paris 2024 a montré que, face aux cybermenaces, la France est capable de conjuguer innovation, expertise et coordination pour garantir la sécurité de ses infrastructures stratégiques.

Le mot de Salah SADOU, porteur de la chaire Cybersécurité des Grands Evénements Publics.

Maintenant, il est question de pérenniser et faire évoluer ce capital expérience acquis grâce à l'organisation de ces jeux. Cela ne peut pas se faire sans une recherche active dans le domaine de la cybersécurité des grands événements publics. C'est cette opportunité qu'offre la Chaire Cybersécurité des Grands Evénéments Publics, de l'Université Bretagne Sud, aux acteurs publics et privés afin de continuer à anticiper l'avenir.

REMERCIEMENTS

La chaire cybersécurité des grands événements publics tient à remercier chaleureusement :

- Les intervenant.e.s
- Le GICAT, mécène de la chaire
- La Gendarmerie Nationale, partenaire de la chaire
- Les personnes présentes lors de cette conférence
- Et les équipes de la Maison de la Bretagne

cyber sécurité : Chaire grands événements publics

Fondation Université Bretagne Sud

Fondation : Université Bretagne Sud

GICAT
Groupement des industries françaises de défense et de sécurité terrestres et aéroterrestres

Contact Chaire Cybersécurité des Grands Événements Publics :
Salah SADOU - porteur de la chaire
salah.sadou@univ-ubs.fr

Fondation Université Bretagne Sud
fondation@univ-ubs.fr
www-fondation.univ-ubs.fr