NEWSLETTER

Juin 2024

JO 2024

DERNIERE LIGNE DROITE

Evènement majeur dans le monde du sport, les Jeux Olympiques et Paralympiques de Paris vont faire rêver des millions de spectateurs et téléspectateurs. Derrières les prouesses sportives se cachent une véritable prouesse technologique pour traiter et diffuser un volume considérable de données en temps réel partout dans le monde.

Mais les JO sont également une énorme vitrine pour tous les pirates désireux de porter atteinte à la France, son image, son économie. Même si certaines structures sont plus susceptibles d'être visées que d'autres, toutes les entreprises françaises, quels que soient leur activité, leur positionnement géographique et leur taille, sont des cibles potentielles.

Aussi, il est primordial de renforcer la sécurité de votre système d'information. InfoPRO vous communique les dernières recommandations de Cybermalveillance.

LES JEUX EN CHIFFRES

DES CHIFFRES A LA HAUTEUR DE L'EVENEMENT

Les Jeux Olympiques et Paralympiques de Paris se dérouleront du 26 juillet au 8 septembre 2024. Un évènement historique avec des chiffres à donner le vertige :

- 9 milliards d'euros de budget ;
- 1 milliard de téléspectateurs attendus pour la cérémonie d'ouverture ;
- 13 millions de repas servis ;
- 30.000 policiers et gendarmes ;
- 15.000 militaires ;
- 17.000 à 22.000 agents de sécurité privée ;
- 10.500 athlètes en provenance de 203 nations ;
- 30.000 volontaires ;
- 6.000 contrôles anti-dopage ;
- 3 à 4 milliards de cyberattaques attendues….

De quoi perdre la tête…

DERRIERE LE SPORT, LA TECHNOLOGIE

L'IT OMNIPRESENTE AUX JO

Souvent méconnu du grand public, l'IT joue un rôle essentiel dans le bon déroulement des JO. En effet, derrière les moments d'émotions sportives se cache toute une chaîne technologique pour capter, remonter, traiter, afficher la donnée et la distribuer au public des stades et aux centaines de millions de téléspectateurs à travers le monde...

Pour les JO 2024, le budget IT est de plus de 500 millions d'euros avec quelques :

- 6 000 écrans géants ;
- 7 000 points d'accès Wi-Fi ;
- 10 000 postes de travail ;
- 384 400 km de fibre optique (ce qui représente la distance Terre-Lune) ;
- 200 applications ;
- 100 serveurs.

Mais les Jeux sont également l'occasion de promouvoir des technologies émergentes telles que :

- La vidéo de surveillance algorithmique qui utilise l'intelligence artificielle pour assurer la sécurité des différentes manifestations
- Les talkies-walkies classiques seront remplacés par le push to talk, une application mobile permettant des appels de groupe instantanés sans composer de numéro, en appuyant simplement sur un bouton sur le téléphone.
- L'IA (Intelligence Artificielle) a été également été utilisée pour l'affectation des bénévoles afin de faire matcher les besoins avec les personnes les plus adaptées.

LES FILETS DU CHALUT DE CYBER-ATTAQUES

CYBERATTAQUES : TOUS CONCERNES !

A quelques jours du coup d'envoi des JO, il est primordial pour toutes les entreprises de renforcer la sécurité de leur système d'information, même si certaines semblent plus exposées que d'autres.

Ainsi, le Comité d'Organisation des JO, les secteurs du transport, de l'énergie, les banques, les télécommunications mais aussi les sponsors officiels sont des cibles de 1er choix.

A cela, s'ajoutent les entreprises indirectement concernées par les jeux, et notamment le tourisme (dont les sites des différents monuments de Paris), l'hôtellerie & les hébergements temporaires, la restauration, les sites de co-voiturage sans oublier les sociétés de pari électroniques.

Enfin, les entreprises dont les bureaux ou le siège social ou un bâtiment important se trouve dans une zone à proximité d'un événement sont également en 1ère ligne.

Bien que seules 30 % des entreprises françaises soient directement concernées, « de nombreuses autres se verront malheureusement prises dans les filets du chalut de cyber-attaques » pour reprendre l'expression de Michel Juvin dans le magazine numérique Alliancy.

Le risque est d'autant plus élevé que :

- un rapport sénatorial de 2021 a suggéré de montrer « l'excellence de la filière française de la cybersécurité » durant les JO, ce qui pourrait être perçu comme un défi par les cybercriminels ;
- le contexte géopolitique actuel fait craindre des attaques cyber menées par des activistes

Les entreprises doivent donc mettre en place des mesures préventives solides.

DERNIERE LIGNE DROITE POUR SECURISER LES RESEAUX

RENFORCER LA SECURITE DE SON SYSTEME D'INFORMATION, UNE NECESSITE ABSOLUE

Face à une menace cyber inégalée pendant la période des Jeux, les entreprises doivent se préparer. Voici les dernières recommandations de cybermalveillance à réaliser avant le coup d'envoi :

- Renforcez la sécurité des accès extérieurs à votre réseau informatique interne notamment en vérifiant les règles de filtrage de vos pare-feu, renforçant la solidité des mots de passe, privilégiant l'emploi d'une double authentification, utilisant des connexions sécurisées via des VPN… ;
- Augmentez la fréquence de sauvegarde de tous vos systèmes et applications critiques en en gardant des copies déconnectées et en vérifiant le bon fonctionnement de leur restauration ;
- Assurez-vous de la bonne mise à jour des correctifs de sécurité de tous vos équipements, et en particulier ceux directement exposés sur Internet (points d'accès extérieurs, VPN, pare-feu, site Internet…) ;
- Utilisez un antivirus à jour sur l'ensemble de vos postes de travail et serveurs ;
- Éteignez si possible vos serveurs, systèmes de sauvegarde en ligne et postes de travail en dehors de plages d'activité normale de votre organisation (ex : nuit, week-end, jours fériés…) ;
- Réalisez une revue de la sécurité de votre site Internet ;
- Renforcez la sécurité de vos comptes de réseaux sociaux ;
- Sensibilisez l'ensemble de vos collaborateurs aux risques et rappelez les consignes de sécurité ;
- Actualisez et vérifiez vos plans de crise en cas de cyberattaque.

Vous ne savez pas par où commencer, vous avez des doutes sur la résilience de votre système, InfoPRO45 peut vous accompagner pour renforcer la sécurité de votre réseau.