# 4 milliards de cyberattaques attendues pendant les JO

*Les JO de Paris 2024 attirent l'attention sur le tissu économique français. 4 milliards de cyberattaques pourraient avoir lieu pendant les Jeux. Il n'est pas trop tard pour protéger votre entreprise.*

Temps de lecture : minute

*18 juillet 2024*

La cérémonie d'ouverture des Jeux Olympiques et Paralympiques de Paris 2024 se tient dans 8 jours et il n'est pas encore trop tard pour préparer son entreprise aux cyberattaques attendues. Mais il faut faire vite. Selon l'organisation de Paris 2024, 4 milliards de cyberattaques pourraient intervenir durant les quinze jours de compétition. Ces cyberattaques peuvent viser des institutions et des parties prenantes dans l'organisation des Jeux, mais aussi des entreprises. «*Les secteurs essentiels comme l'eau, l'électricité, les transports pourront être visés*», analyse Julien Lopizzo, PDG de Semkel, un cabinet de sécurité économique.

«*Tous les événements vitrines sont cibles d'attaques*», confirme Jérôme Calmelet, président de Kyndryl. «*La plupart des entreprises ne sont pas prêtes mais il n'est pas trop tard*», insiste Julien Lopizzo.  Quels sont les bons gestes à adopter pour se protéger ? D'abord, installer un anti-virus, faire des sauvegardes de ses données. Cela peut paraître évident mais fera la différence en cas de tentatives d'attaques ou d'attaques. On peut également faire appel à un SOC : un Security operating partner. Julien Lopizzo donne un autre conseil plus radical : «*Si votre entreprise ferme pendant l'été, débranchez tous vos serveurs non essentiels. Il ne suffit pas de les éteindre ou de les mettre en veille.*»

# Des nouveaux types d’attaques

En effet, l’analyste spécialiste des risques économiques note une recrudescence des attaques dites silencieuses. Le virus vient se loger dans les systèmes informatiques de manière indolore de l’entreprise et ne se déclare que plusieurs jours ou mois plus tard. Julien Lopizzo note également le retour des ransomwares, ces cyberattaques qui prennent vos données en otage contre une rançon. Jérôme Calmelet alerte sur un nouveau type d’attaques permis par l’intelligence artificielle. Avec les deepfakes, les attaquants peuvent se faire passer pour le président ou le DG de l’entreprise visée.

«*Vous recevez un message de votre président d'entreprise disant ‘j’ai une information strictement confidentielle à partager avec vous, veuillez vous connecter à ce lien à 16 heures dans l'après-midi.’ Là, vous allez avoir une vidéo de votre président qui vous demande d’aller voir votre directeur financier pour faire un certain nombre de transferts parce que vous voulez faire une acquisition locale, mais comme c'est confidentiel, il ne faut surtout pas partager cette information. Votre président vous parle en visio générée par l'intelligence artificielle. Il y a quelques mois, quelques années, cela n’existait pas. Donc quand vous êtes en visio avec quelqu'un qui a la même voix, la même intonation, qui peut interagir, cela crée des doutes et une certaine pression sur les employés.Ce genre d’attaques arrivent régulièrement.*» Il faut donc faire de la prévention !

# La résilience cyber

Dans ce sens, il est essentiel de réduire au maximum le risque d’attaques *«en évitant d’avoir les fenêtres ouvertes, les portes ouvertes»*, image Jérôme Calmelet. *«Cela passe par de la prévention auprès de chaque collaborateur de la société. C’est dans leur quotidien : ils sont sous stress, sous pression dans leur travail, ils reçoivent un SMS en disant ‘votre colis n'a pas pu être livré, veuillez cliquer sur ce lien-là, vous êtes en pleine*

*réunion, les enfants ne sont pas à la maison, voilà.' Et donc les gens cliquent. C'est un vrai travail d'évangélisation.»*

Si on se retrouve dans une telle situation, que faire ? *«Tout le monde va être attaqué et à un moment donné, l'attaque va gagner»*, insiste le président de Kyndryl. «*Le plus important est que l'impact soit mineur pour l'entreprise et de pouvoir redémarrer au plus vite. C'est ce qu'on appelle la cyber-résilience*.» Chaque structure doit mettre en place un plan de reprise d'activité scriptant la marche à suivre pour récupérer ses données. Il faut bien sûr cartographier ses datas et investir dans un cloud de secours pour les sauvegarder. *«Les entreprises nous disent que cela coûte cher de se protéger. Mais c'est encore moins cher que de se préparer à devoir redémarrer avec des sarcophages et autres protections»*, conclut Jérôme Calmelet.

À lire aussi
Cybersécurité : un startup studio lancé au Campus Cyber pour propulser 10 pépites européennes en 5 ans


# MADDYNEWS

La newsletter qu'il vous faut pour ne rien rater de l'actualité des startups françaises !

JE M’INSCRIS

---

Article écrit par Aurélie Pasquier