TERRITOIRES D'ÉVÉNEMENTS SPORTIFS.

Note de synthèse

Les enjeux Cybersécurité pour Paris 2024

1. SYNTHESE

Lors de l'organisation d'un grand événement international, comme les Jeux Olympiques et Paralympiques ou la Coupe du Monde de Rugby, la question n'est plus de savoir si la manifestation sera sujet ou non à des cyberattaques mais désormais quand et comment.

Les autorités étatiques s'attendent à ce que le nombre d'attaques augmentent très fortement à l'occasion de Paris 2024 comparativement aux Jeux Olympiques de Tokyo en 2021.

Les collectivités territoriales hôtes, en raison de leur visibilité, pourraient aussi être la cible d'attaques malveillantes.

Dans le dispositif actuel de Paris 2024, c'est la collectivité hôte qui est responsable de son périmètre et doit donc mettre en place une sécurisation de ses systèmes d'information comme de ses infrastructures sportives.

En s'inspirant des recommandations prônées par l'Etat, la collectivité hôte doit donc prendre les mesures adéquates, et consacrer des moyens humains et budgétaires suffisants, pour garantir sa cybersécurité.

Il lui faudra notamment :

- Sensibiliser l'ensemble de ses élus, dirigeants et agents, et dépasser un fonctionnement classique reposant uniquement sur les services et directions informatiques pour un travail plus collaboratif impliquant l'ensemble des directions
- S'entourer des bonnes compétences, techniques ou organisationnelles, en interne et/ou en externe ;
- Procéder à une analyse de risque liée aux Jeux, conduisant à un planning de scénarios ;
- S'équiper en conséquence à l'état de l'art ;
- Mettre en place un process de détection de la menace ;
- Construire un plan de reprise d'activité pour assurer sa résilience.

La Collectivité devra s'attacher à inclure en amont la cybersécurité dans toutes ses activités liées aux Jeux (*secure by design*).

Les Jeux Olympiques et Paralympiques représentent donc aussi une opportunité pour les collectivités hôtes, de mettre en place, ou à jour, leur système de cyberdéfense, leur permettant d'anticiper les attaques, avant, pendant et après les Jeux.

Cette progression peut alors constituer un héritage de Paris 2024 face à une menace qui perdurera.

2. INTRODUCTION

Un grand événement sportif international est un reflet des évolutions technologiques de la société. Il est devenu naturellement un événement connecté, connecté à son temps, connecté à son public, connecté à sa ville, connecté au monde.

Aussi l'aspect cybersécurité est-il devenu indissociable de l'organisation d'un grand événement, comme les Jeux Olympiques et Paralympiques de Paris 2024 ou la Coupe du Monde de Rugby 2023. Leur visibilité mondiale et leurs enjeux multiples, provoqueront donc une cybermenace accrue, pouvant venir de partout et sous différentes formes.

Les organisateurs de l'événement et leur écosystème, mais aussi l'Etat et les collectivités locales qui accueillent ces événements, sont donc tous concernés.

La menace pèsera non seulement sur le bon déroulement des épreuves, mais pourra aussi mettre à risque le bon fonctionnement et l'image des collectivités hôtes, dont la visibilité sera accrue.

Récemment leur surface d'exposition a d'ailleurs déjà augmenté, que ce soit avec la transformation numérique de la ville, la connectivité des infrastructures sportives et l'apparition des objets connectés.

Dès lors, Il ne s'agit plus de savoir si la collectivité sera attaquée mais plutôt également quand et comment …

Pour affronter ces défis, elle doit donc anticiper dès maintenant et :

- Se préparer en amont ;
- Penser au facteur humain, en sensibilisant et mettant en place une approche collaborative favorisant la communication interne sur le sujet ;
- S'attendre à tous types de menaces ;
- Travailler sa résilience.

Les bonnes pratiques et les expertises pour se protéger existent.

Pour réagir correctement en cas d'attaque, il est alors nécessaire de mettre le sujet de la cybersécurité au bon niveau de priorité d'y consacrer les moyens adéquats

3. LES PRINCIPAUX OBJECTIFS DE LA STRATEGIE CYBERSECURITE DE PARIS 2024

3.1. L'enjeu d'image

La France se doit d'afficher au monde sa maîtrise de l'organisation d'événements internationaux, des technologies, et laisser aux accrédités comme au grand public, un souvenir inoubliable de leur expérience.

3.2. L'enjeu organisationnel & opérationnel

Face aux cybermenaces de tous types, il s'agit d'assurer le bon déroulement des Jeux Olympiques et Paralympiques (ainsi que de la Coupe du Monde de Rugby), que ce soit au niveau des compétitions sportives, des manifestations les entourant (cérémonies d'ouverture, de clôture ou les célébrations), de la couverture médiatique, des transports, etc.

Le dispositif de cybersécurité devra donc contribuer à :

- Garantir la sécurité de l'ensemble des populations concernées (public, athlètes, juges arbitres, officiels, journalistes, bénévoles …) ;
- Protéger les biens et les sites ;
- Assurer le bon déroulement des épreuves ;
- Assurer la bonne communication autour de l'événement ;
- Préserver l'image des organisateurs et des villes hôtes ;
- Garantir des opérations de cybersécurité optimales.

3.3. L'enjeu d'héritage

Enfin, les JOP seront une opportunité pour la collectivité hôte de mettre en place un système de cybersécurité qui constituera un héritage après 2024.

4. GRANDS PRINCIPES EN MATIERE DE CYBERSECURITE

La cybersécurité permet de protéger les données et l'intégrité des ressources informatiques et télécoms connectées à un événement contre toutes les malveillances informatiques.

4.1. Périmètre

Alors que la sécurité traditionnelle permet de délimiter des périmètres physiques de responsabilité (l'organisateur au sein de l'enceinte, l'Etat en dehors), la cybersécurité échappe à cette logique. Les frontières y sont en effet beaucoup plus floues dans un écosystème d'entités interconnectées.

4.2. Approche

Cependant l'approche à mettre en place pour la cybersécurité s'apparente à celle de la sécurité physique :

Il s'agira donc de :

- Connaitre le périmètre de sa responsabilité, ses forces et ses faiblesses ;
- Déterminer les différents périmètres susceptibles d'être attaqués ;
- Evaluer les risques correspondants ;
- Mettre en place des protections adéquates et les faire évoluer ;
- Détecter les menaces au fil du temps ;
- Prévoir les plans d'action pour se défendre en cas d'attaque.

Le sujet est d'autant plus complexe à couvrir que :

- Les technologies évoluent sans cesse ;
- Les surfaces exposées augmentent ;
- Les menaces sont plus nombreuses et de plus en plus sophistiquées.

4.3. Typologie des menaces

D'ici 2024, les menaces vont encore évoluer et prendront de nouvelles formes :

a. Quelles cibles ?

Jusqu'à présent, les systèmes d'information (IT : Information Technology) étaient la cible de la plupart des attaques, par des intrusions sur les réseaux ou sur les postes de travail. Désormais les réseaux industriels et opérationnels (OT : Operationnal Technology) composés d'objets connectés sont aussi ciblés). L'organisation des JOP et son écosystème

seront visés, y compris les collectivités qui les hébergent, en exploitant leurs vulnérabilités (IT et OT).

b. Origine des menaces

Aujourd'hui elles peuvent provenir d'Etats, de groupes criminels, de terroristes, d'hacktivistes (activistes d'une lutte militante à dimension politique, religieuse ou sociale.) ou encore d'officines spécialisées. Il existe aussi un marché de revente du rançongiciel où des amateurs peuvent se fournir.

c. Dans quel but ?

Saisir l'opportunité d'un grand événement comme les JOP ou la Coupe du Monde de Rugby à des fins de déstabilisation, de gain financier, de sabotage voire d'espionnage.

4.4. Type d'attaques classiques

Les menaces les plus courantes aujourd'hui concernent les systèmes d'information :

a. Logiciels malveillants (malware)

Logiciels indésirables qui sont installés dans votre système sans votre consentement. Des hackeurs, des organisations mafieuses ou même des gouvernements s'en servent pour voler des renseignements, pour chiffrer ou supprimer des données sensibles, modifier ou détourner les fonctions du système attaqué ou espionner.

Parmi les malwares se trouvent notamment :

- Les chevaux de Troie, les plus courants avec 20% des attaques[1]. Ils ouvrent une porte d'entrée clandestine (backdoor) dans votre ordinateur pour donner l'accès à des programmes ou utilisateurs malveillants, et dérober les informations personnelles et confidentielles ;
- Les « wiper » qui effacent toutes les données des disques durs ;
- Les attaques par « chaine d'approvisionnement logiciel » qui injectent des composants logiciels malveillants dans un produit sans que l'éditeur ou le client final ne s'en aperçoive.

A l'occasion des JOP, les malwares peuvent provoquer l'indisponibilité d'un site internet, de la connexion internet d'un stade, de son système de vidéosurveillance, du wifi, de l'affichage dans le stade et/ou de la diffusion de flux vidéo.

b. L'hameçonnage (phishing)

L'hameçonnage (phishing) vous envoie des courriels qui semblent provenir de sources fiables dans le but d'obtenir des informations ou de vous inciter à mener une action. Les JOP de Tokyo 2020 ont été la cible de nombreux actes d'hameçonnage utilisant le thème des Jeux pour escroquer les citoyens (vente de faux billets par courriel, extorsion…).

[1] *Rapport Cisco Talos Incident Response, Juillet 2022*

c. Le rançongiciel (ransomware)

Le rançongiciel (ransomware) est un malware qui exige un paiement pour ramener le système attaqué à son état normal. Le hackeur, après avoir récupéré un login et un mot de passe, accède à une ressource de la collectivité puis augmente ses privilèges et déploie sur l'ensemble du parc le rançongiciel. Au deuxième trimestre 2022, ils représentent 15 % de toutes les menaces observées contre 25 % au premier trimestre[2]. Cette baisse est due à plusieurs facteurs tels que les récents démantèlements de groupes de ransomwares par les forces de l'ordre (ex : ComCyberGend).

Les exemples de collectivités ou d'administration publique s'étant faites rançonner sont nombreux. Le dernier en date concerne le CHU de Corbeil-Essonnes. Il a été refusé de payer les 10 millions de dollars qui lui étaient demandés. Depuis, une partie des données des usagers, personnel et partenaires ont été divulguées sur le darknet.

d. Attaques par déni de service (DOS ou DDOS)

Les attaques par déni de service sont des cyberattaques, émanant d'une ou de plusieurs sources, qui saturent un système, afin que ce dernier ne puisse plus répondre, en l'inondant de trafic malveillant. Très récemment, Google a révélé avoir bloqué un assaut de plus de 46 millions de requêtes par seconde le 1er juin 2022, ce qui constitue un record…

- Les sites web sont souvent les premiers concernés ;
- Une infrastructure sportive peut aussi en être victime et compromettre le bon déroulement d'une épreuve (système électrique par exemple).

e. Défigurations/défacement de sites web

Le pirate modifie l'apparence ou le contenu d'un site web, en y associant un message ou une revendication. Cela peut concerner par exemple le Site internet des collectivités.

4.5. Evolution des attaques

Tout d'abord les attaques sont de plus en plus sophistiquées avec d'importants moyens financiers déployés. Ces attaques évoluent aussi avec un environnement qui change :

- Les systèmes d'information jusque-là plutôt centralisés et dans des périmètres fermés, ont eu tendance à s'ouvrir (ex : télétravail) ;
- Une adoption rapide du cloud où se trouvent de plus en plus d'applications et de données ;
- Une multiplication du nombre d'objets connectés à des réseaux de tous types ;
- Des bâtiments, des usines, des infrastructures sont maintenant aussi connectés ;
- Un usage des réseaux sociaux de plus en plus intense.

Les nouvelles menaces s'étendent donc au-delà des systèmes d'information classiques (IT) et concernent donc désormais les réseaux opérationnels (OT) des stades, les réseaux de caméras de surveillance, les circuits d'affichage, d'éclairage, les stations d'épuration d'eau, les centrales électriques etc. qui peuvent se retrouver paralysés.

[2] *Rapport Cisco Talos Incident Response, Juillet 2022*

Parmi ce nouveau type d'attaques, on peut citer des attaques :

- Sur des réseaux électriques en Europe de l'Est, ayant conduit à des coupures totales d'électricité de plusieurs jours ;
- Le vol de 110 millions de cartes bancaires d'une chaîne de magasins américains, que les pirates ont réussi à pénétrer, via une faille dans le réseau de gestion des systèmes de ventilation ;
- Ou encore un réseau d'eau potable américain victime d'une attaque durant laquelle les cybercriminels ont eu accès au système de dosage de produits chimiques nécessaires pour assainir l'eau.

Il faut également citer les attaques interconnectées très appropriées à un GESI (Grand Evénement Sportif International).

Elles peuvent provoquer des réactions en chaine, de la même manière qu'en sécurité physique (Cf. événements du Stade de France lors de la finale de la Ligue des Champions). Un grand événement doit en effet être considéré comme un *système de systèmes*[3].

Il est indispensable de sécuriser tous les éléments séparés de la chaîne pour assurer la résilience de l'événement. Les attaquants chercheront à rentrer par le maillon faible. Ainsi, l'attaquant peut lancer une attaque indirecte pour accéder à la cible finale. Un attaquant tentera donc par exemple de diriger son attaque contre la partie A, l'objectif final étant une attaque contre la partie B. D'où l'importance d'une collaboration accrue entre toutes les parties prenantes.

L'exemple du stade :

Un stade abrite aujourd'hui différents dispositifs informatiques au service des exploitants, des organisateurs d'événements, du public et des partenaires. La cybersécurité d'un stade, se rapproche aujourd'hui de la gestion du risque cyber dans le monde industriel.

En effet on y trouve pour commencer, des réseaux câblés locaux, du wifi, de la fibre et de la 4G et bientôt de la 5G, servant des applications sensibles (gestion des accès par exemple).

Le stade comporte aussi des réseaux dédiés à la gestion technique des bâtiments et des infrastructures (contrôle d'accès, climatisation, chauffage, ventilation, alimentation électrique, automatismes, sécurité incendie, etc.) mais aussi un réseau de caméras de surveillance.

Les risques peuvent aller de l'arrêt de l'équipement (arrêt de la climatisation, coupure de courant, déclanchement de l'alarme incendie, etc.) à sa reconfiguration complète (mise en route du chauffage en plein été) pouvant conduire à sa destruction (surchauffe puis explosion d'un convertisseur électrique).

L'exemple de la Coupe du Monde de football au Qatar sera intéressant à suivre, sachant que la climatisation sera critique pour le bon déroulement de l'épreuve.

Par nature, ces systèmes de type industriel sont peu ou pas protégés, les personnes les mettant en œuvre n'ayant pas toujours une *culture cybersécurité*.

[3] *Sujet de recherche de la chaire Cybersécurité des grands évènements de l'Université Bretagne Sud de Vannes.*

Par ailleurs, comme ces réseaux sont connectés au reste de l'installation, le risque est fort qu'ils deviennent également une porte d'entrée vers le reste du système informatique.

4.6. Le principe de résilience en cybersécurité

La résilience est une pierre angulaire de la cybersécurité. La capacité de pivoter rapidement tout en maintenant la continuité des activités et des défenses robustes est de plus en plus importante dans le monde d'aujourd'hui.

Les menaces existent et des incidents se produisent. La résilience est atteinte lorsque la probabilité qu'un incident se produise est réduite et que l'impact causé est minimisé.

Le fondement d'une résilience réussie vient de la compréhension des menaces et de vos propres faiblesses. Armé de ces connaissances, vous pouvez mettre en œuvre des protections pour réduire la probabilité que les menaces vous affectent et vous assurer que si une menace se réalise, les effets seront minimisés.

Un autre élément important de la résilience est la capacité non seulement d'identifier quand quelque chose ne va pas, mais aussi de le faire rapidement. Il s'agit de concepts connus sous le nom de temps moyen de détection (MTTD) et de temps moyen de réponse (MTTR).

L'exemple du Superbowl aux USA (70000 personnes) au stade SOFI de Los Angeles, 110 Millions de téléspectateurs :

« *Le Super Bowl et des événements de cette ampleur nécessitent une orchestration gigantesque de l'interconnexion, non seulement du point de vue de la technologie, mais aussi du point de vue des personnes* », a déclaré Tomás Maldonado, directeur de la sécurité de l'information de la NFL. « *Ce que nous essayons de faire, c'est de ralentir les mauvais acteurs et de rendre plus difficile pour eux de nous attaquer et d'avoir un impact sur ce qui se passe sur le terrain. Mais en même temps, nous devons également regarder au-delà du terrain et penser à toutes les différentes parties de notre entreprise qui pourraient être touchées par une attaque, en reconnaissant que nos facteurs de risque changent constamment.* ».

5. PRINCIPAUX ACTEURS ET RESPONSABILITES

A ce jour, la convention hôte type qui régit les relations entre le COJOP et les collectivités territoriales n'aborde pas le sujet de la cybersécurité, en termes de droits et devoirs.

Il existe un protocole de sécurité entre l'Etat et Paris 2024, mais qui ne concerne pas les collectivités territoriales. La stratégie cybersécurité y est définie par le ministère de l'Intérieur et l'ANSSI (mars 2022).

L'État joue un rôle de pilote via la Délégation Interministérielle aux Jeux Olympiques et Paralympiques (DIJOP), chargée de conduire la planification et la livraison opérationnelle des engagements de l'Etat, qui s'appuie sur la Coordination Nationale pour la Sécurité des Jeux (CNSJ) pour l'ensemble des sujets relevant de la sphère de compétence du ministère de l'Intérieur.

La gouvernance relative aux questions de cybersécurité des JOP, de façon simplifiée est la suivante :

5.1. La DIJOP (Délégation Interministérielle aux Jeux Olympiques et Paralympiques)

Les missions de la Délégation Interministérielle aux Jeux Olympiques et Paralympiques sont les suivantes :

- Conduire la planification et la livraison opérationnelle des engagements de l'Etat ;
- Animer et coordonne les activités des administrations et établissements publics nationaux concourants à l'organisation des JOP 2024 ;
- Suivre l'avancement des projets portés par la SOLIDEO ;
- Elaborer des propositions de dispositions législatives et réglementaires pour les JOP 2024 ;
- Assurer les relations de l'État avec le COJOP et, en liaison avec les Préfets, avec les collectivités territoriales ;
- Piloter le programme d'héritage du Gouvernement

En matière de sécurité, le DIJOP s'appuie sur le Coordonnateur National pour la Sécurité des Jeux (CNSJ) qui lui est rattaché fonctionnellement.

5.2. La CNSJ (Coordination Nationale de la Sécurité des Jeux Olympiques et Paralympiques)

La CNSJ, qui dépend du ministre de l'Intérieur initie, anime et coordonne en matière de cybersécurité, toutes les activités de son périmètre qui concourent à l'organisation des Jeux 2024 et à tous les événements sportifs internationaux. Dans ce cadre, elle veille, en étroite collaboration avec les préfectures concernées, à la planification et la mise en œuvre des opérations de sécurité et de sûreté, y compris donc de cybersécurité. Elle anime un réseau regroupant l'ensemble des acteurs concernés par la cybersécurité des Jeux, dont les collectivités hôtes, afin de les informer sur l'Etat de l'Art, l'état de la menace, des indicateurs de compromission (élément d'investigation numérique qui indique qu'un terminal ou un

réseau a été compromis4…). Lui est rattaché structurellement le Centre de Renseignement Olympique (CRO).

Le Centre de Renseignement Olympique (CRO) a été mis en place au printemps 2021, à l'approche de la Coupe du Monde de Rugby 2023 des Jeux Olympiques et Paralympiques 2024 pour contribuer à leur sécurité.

Il a pour objectif le développement de la connaissance et des capacités d'anticipation.

Le CRO a vocation à prendre en compte l'ensemble du spectre des menaces (y compris cybermenaces) pesant ces événements, afin de permettre aux autorités administratives, aux dispositifs de sécurité intérieure et de sécurité civile d'anticiper et, de disposer d'une autonomie d'appréciation, de décision et d'action,

Il centralise, analyse, et diffuse le renseignement relatif à la connaissance et à l'anticipation des risques et à la détection des menaces pouvant impacter l'événement.

Le CRO s'appuie sur tous les services de la communauté française du renseignement, mais également l'ensemble des services et unités des DGPN et DGGN (le ComCyberGend).

Le CRO, centre interservices, interministériel et à vocation internationale, établit un lien direct avec le centre de veille du ministère de l'Intérieur, le ministère des Armées ainsi que pour les services du Premier ministre le SGDSN et l'ANSSI, ainsi que les collectivités territoriales impliqués.

Sa mise en place s'est faite de manière progressive depuis 2021. Il fonctionnera 7 jours sur 7 en H24, pendant la coupe du monde de rugby et 100 jours avant le début des jeux olympiques de Paris 2024 (relais de la flamme olympique – 15 avril 2024).

Le CRO est rattaché fonctionnellement au coordonnateur national du renseignement et de la lutte contre le terrorisme.

[4] *1er séminaire organisé par la CNSJ le 20 juin 2022*

5.3. Le COJOP PARIS 2024

Le COJOP (Comité d'Organisation des Jeux Olympiques et Paralympiques) est responsable du bon fonctionnement du système d'information des Jeux Olympiques et Paralympiques et de sa sécurisation.

Par système d'information des JOP, on entend :

Le système d'information du COJOP en tant qu'entreprise traditionnelle, mais aussi son extension installée de manière éphémère pour couvrir les épreuves dans les enceintes sportives.

Il permet l'interconnexion des sites olympiques officiels (stades, sites provisoires, villages olympiques et médias,), autorise l'accès sécurisé à l'information et son traitement à toutes les personnes accréditées (personnel COJOP, officiels, prestataires,) depuis les sites olympiques.

Les systèmes et réseaux installés par le COJOP, dans les stades existants et possédant déjà leur propre système d'information, sont éphémères et en « *overlay* » (en superposition des systèmes existants).

Le COJOP supervise les installations éphémères sur site (réseau,) et doit s'assurer de la mise à niveau des acteurs avec qui il travaille (cf. EDE ci-dessous)

Exemples d'éléments sensibles du Système d'Information à sécuriser par le COJOP :

- Confidentialité des données personnelles (athlètes, public, officiel, bénévoles…) ;
- Disponibilité et intégrité des applications ;
- Site internet et billetterie ;
- Applications mobiles (grand public, athlètes…).
- Au sein des enceintes sportives olympiques :

    - Connectivité, réseau du stade ;
    - Gestion des accès ;
    - Gestion des accréditations ;
    - Gestion technique du bâtiment (électricité, eau, ventilation sécurité incendie, ascenseurs) => alarmes, conso, pilotage à distance ;
    - Collecte des données dans le stade ;
    - Contrôle d'accès spectateurs (tripodes, PDA, connectés au pc de contrôle en wifi ou en 5g) ;
    - Réseaux de caméras ;
    - Chronométrage, résultats ;
    - Affichage, sonorisation ;
    - Systèmes d'éclairage ;
    - Services aux spectateurs.

5.4. La SOLIDEO (Société de Livraison des Ouvrages Olympiques)

La SOLIDEO est responsable de la sécurisation des installations du village Olympique, et du village des médias.

5.5. L'EDE (Event Delivery Entity)

Pour rappel, c'est une entreprise ou un groupement choisi par le COJOP en tant que délégataire de l'organisation d'une compétition sportive et/ou de la gestion du site où elle se déroule.

Le COJOP lors de l'attribution du marché à l'EDE, doit s'assurer de la maturité de celle-ci et de ses compétences cyber en vue d'appliquer une démarche cybersécurité « Etat de l'art » au périmètre qui lui est confié.

Un travail conjoint sera cependant mené entre le COJOP et l'EDE sur les aspects communs, voire aussi avec le propriétaire du site en bonne intelligence.

5.6. Partenaires et acteurs majeurs du COJOP en matière de cybersécurité

- **Cisco** (partenaire TES) est Partenaire Officiel des infrastructures de cybersécurité de Paris 2024 (et fournit aussi les équipements réseaux et les logiciels de visioconférences).
- **Atos** est le fournisseur officiel du système d'information du Comité International Olympique (Partenaire IT mondial), mais est également le Supporteur Officiel en services et opérations de cybersécurité. A ce titre il est notamment responsable du Cyber SOC de Paris 2024 :
  - SOC : Security Opération Center (Centre des opérations de Sécurité)
  - Ce cyber SOC agrège toutes les remontées d'information de cybersécurité du terrain et est connecté aux centres de cybersécurité étatiques.
- **Orange** est le partenaire qui installe et opère le réseau olympique dans les stades, et à ce titre est responsable du « NOC » (Network Operation Center - Centre des opérations Réseaux).
- **OBS** (Olympic Broadcasting Systems) est responsable de la Captation et Diffusion des images (flux vidéo…).

5.7. ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) :

L'ANSSI est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Elle propose au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant l'intégrité numérique de la Nation et coordonne l'action gouvernementale en matière de défense des systèmes d'information. Elle anime, coordonne les travaux interministériels en matière de sécurité du numérique et élabore les mesures de protection des systèmes d'information, en veillant à l'application de celles-ci notamment par le biais d'audits.

Depuis juillet 2022, le pilotage de la stratégie de prévention des cyberattaques en vue des Jeux est confié à l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Dans l'objectif, d'une part, d'avoir sécurisé début 2024 les systèmes critiques pour la bonne tenue des JOP2024 et, d'autre part, de disposer d'un dispositif opérationnel dédié et éprouvé de gestion des crises cyber, l'action de l'ANSSI, en étroite collaboration avec les différentes structures impliquées dans l'organisation des JOP2024, se structure selon quatre axes d'efforts visant à parfaire la connaissance des menaces cyber pesant sur les Jeux, sécuriser les systèmes d'information critiques, protéger les données sensibles et enfin se préparer opérationnellement à intervenir en cas d'attaque cyber affectant l'événement.

- **OIV (Operateurs d'Importance Vitale) et OSE (Opérateurs de Service Essentiel)**

Les OIV et OSE regroupent les acteurs de la Santé, Transport, Télécom, Eau, Electricité, Gaz, et présents sur le territoire de la collectivité :

Ils ont un régime imposé par le SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale) et sont en prise directe avec l'ANSSI sur les aspects cybersécurité. Leur suivi est continu. Certains OIV/OSE, et notamment dans le domaine des transports ou de l'eau peuvent se trouver sous la responsabilité directe des collectivités qui doivent y apporter une vigilance particulière du fait de leur criticité (ex : régie de transports, d'eau, etc.).

5.8. Collectivités hôtes

Il n'est pas prévu de dispositif particulier en matière de cybersécurité pour les collectivités-hôtes dans le cadre des Jeux.

Elles restent cependant responsables de leur cybersécurité sur leur périmètre traditionnel, notamment sur l'analyse de risque, la détection de la menace, et la remédiation en cas de cyberattaque.

Elles seront donc amenées à prendre en charge notamment :

- La cybersécurité hors du périmètre COJOP sur leurs compétences habituelles ;
- La sécurisation et la communication et l'information aux habitants ;
- La cybersécurité des sites de célébration dont elles auraient la gestion (Live Sites) ;
- La cybersécurité des sites dont elles sont propriétaires qui seront activés pour les Jeux (ex : centre des médias non accrédités à Paris) ;
    - Centres de préparation ;
    - Centres d'entrainement.
- La sécurité des autres événements concomitants pendant les Jeux gérés par elles (ex : manifestations dans le cadre de l'olympiade culturelle).

En cas de cyberattaque(s), le premier niveau est géré par la collectivité (et ses partenaires), avant intervention éventuelle des services de l'Etat (ANSSI, ComCyberGend, DGPN,…).

Elles devront porter une attention particulière à la cybersécurité des installations en place à l'année dans les enceintes dont elle est propriétaire/responsable et auxquelles viendront se connecter le système d'information éphémère du COJOP (en overlay) lors des épreuves.

5.9. Ministère de l'Intérieur

a. Direction Générale de la Gendarmerie Nationale « ComCyberGend »

En dehors de la CNSJ, Le ComCyberGend couvre traditionnellement l'ensemble du périmètre cyber, quelle que soit la nature de la cybervictime. Trois axes prioritaires d'action sont couverts s'agissant des collectivités locales d'une part, des acteurs économiques d'autre part dont les ETI/PME et plus globalement de l'ensemble de nos concitoyens.

Ses 2 activités majeures sont **la prévention et l'investigation en cas de cyberattaques** (7 500 enquêteurs qui passeront à 10 000 en 2024, repartis sur l'ensemble du territoire national y compris l'outre-mer).

En cas de cyber attaques, coté investigation :

S'agissant des ransomwares, la Police Nationale (sous-direction de lutte contre la cybercriminalité), la Gendarmerie Nationale (division des opérations du **ComCyberGend** et ses antennes régionales sur le territoire) et la Préfecture de Police sont chacun chargés d'enquêtes judiciaires sur le sujet suivant les directives du parquet J3 du Tribunal de Grande Instance de Paris, parquet spécialisé dans le domaine cyber et qui dispose d'une compétence concurrente nationale sur les enquêtes touchant le domaine cyber.

ComCyberGend pendant une attaque se déplace sur site auprès de la collectivité et envoie :

- Des experts techniques (qui travailleront de concert avec la société de remédiation) ;
- Des experts de police judiciaire ;
- Des experts gestion de crise (GIGN).

b. Direction Générale de la Police Nationale

La sous-direction de lutte contre la cybercriminalité OCLCTIC **(Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)** est rattachée à la Direction Centrale de la Police Judiciaire.

Elle est composée en central de 150 personnels (policiers, gendarmes, administratifs, ingénieurs, techniciens et contractuels) et elle a pour objectif de lutter contre la cybercriminalité en intégrant les missions d'enquête, d'appui, de détection et de renseignement.

Elle s'appuie sur le réseau territorial des LIONs (Laboratoires d'Investigation Opérationnelle du Numérique), pôles d'excellence hébergés par la PJ et qui viennent compléter le réseau des 500 ICC (investigateurs en cybercriminalité)

Elle apporte donc une réponse judiciaire aux incidents de cybersécurité, en procédant aux enquêtes et à l'investigation numérique en co-saisine ou en assistance, des services de la police nationale, de la gendarmerie nationale et de la DGSI.

S'agissant des rançongiciels elle a une vocation de centralisation et de coordination nationale depuis février 2020. (Elle gère par exemple un inventaire de ransomwares de l'ordre de 150 souches actives)

La sous-direction est aussi en charge des plateformes PHAROS dédiée au signalement et au traitement des contenus illicites de l'Internet ainsi que d'une plateforme de Traitement Harmonisé des Enquêtes et Signalements pour les E-Escroqueries « THESEE », sujets qui pourraient être fortement d'actualité lors des JOP (billets, locations,…).

Lors de la période des JOP, la sous-direction passera en cellule de crise.

c. Préfectures

Elles assurent une animation de l'action publique territoriale en matière de cybersécurité. L'Autorité qualifiée pour la sécurité des systèmes d'information (AQSSI) est le préfet.

6. OBLIGATIONS ET RESPONSABILITES DES COLLECTIVITES TERRITORIALES EN MATIERE DE CYBERSECURITE

6.1. Obligations existantes

Les collectivités territoriales ont un certain nombre d'obligations en matière de cybersécurité :

- Obligations liées à la protection des données personnelles : La collectivité est tenue d'appliquer le Règlement Général sur la Protection des Données ;
- Obligations liées à la mise en œuvre de téléservices locaux ;
- Obligations liées à l'hébergement des données de santé.

Il n'existe donc aucune obligation particulière des collectivités dans le cadre de l'organisation d'un grand événement comme les JOP ou la Coupe du Monde de Rugby.

6.2. Responsabilités

Guide : obligations et responsabilités des collectivités locales en matière de cybersécurité (cnil.fr)

La responsabilité administrative pour faute :

- Traditionnellement, les citoyens peuvent engager la responsabilité de l'administration pour faute lorsque cette dernière a manqué à ses obligations et que le manquement leur a causé un préjudice ;
- À l'avenir, l'application de ce régime de responsabilité pour faute en cas de cyberattaque n'est pas à exclure. Des entreprises ou des administrés pourraient réclamer, auprès d'une collectivité locale ou d'un établissement public, l'indemnisation des préjudices subis du fait des conséquences d'une cyberattaque, s'il peut être établi que les conséquences dommageables de l'attaque sont imputables à des manquements de l'administration dans l'application de la réglementation relative aux systèmes d'information.

Responsabilité civile : la responsabilité personnelle des élus et des agents publics

- La responsabilité civile personnelle des élus et agents publics pourrait, aussi à l'avenir, être engagée en cas de cyberattaque.
- Dans ce contexte, les élus, dirigeants et les agents publics dans les collectivités locales et leurs établissements publics doivent avoir au cœur de leurs préoccupations :
    - le respect des différentes réglementations présentées ;
    - l'analyse préalable des risques pesant sur les systèmes d'information ;
    - la détermination des solutions techniques et organisationnelles.

7. ENSEIGNEMENTS DES JEUX DE TOKYO 2020

Il est évoqué un nombre d'environ 1 milliard d'incidents de cybersécurité constaté aux Jeux de Tokyo 2020[5]. Cependant aucun d'entre eux n'a eu de conséquences majeures.

A titre de comparaison, pour information, durant les Jeux de Pékin en 2008, 12 millions d'incidents liés à la cybersécurité avaient été signalés[6] et 212 Millions à Londres en 2012. Les Jeux Olympiques de Rio de 2016 ont traité plus de 510 millions d'incidents de sécurité[7].

Incident de cybersécurité (définition ANSSI) : Un incident de sécurité est un événement qui porte atteinte à la disponibilité, la confidentialité ou l'intégrité d'un bien. Exemples : utilisation illégale d'un mot de passe, vol d'équipements informatiques, intrusion dans un fichier ou une application, etc.

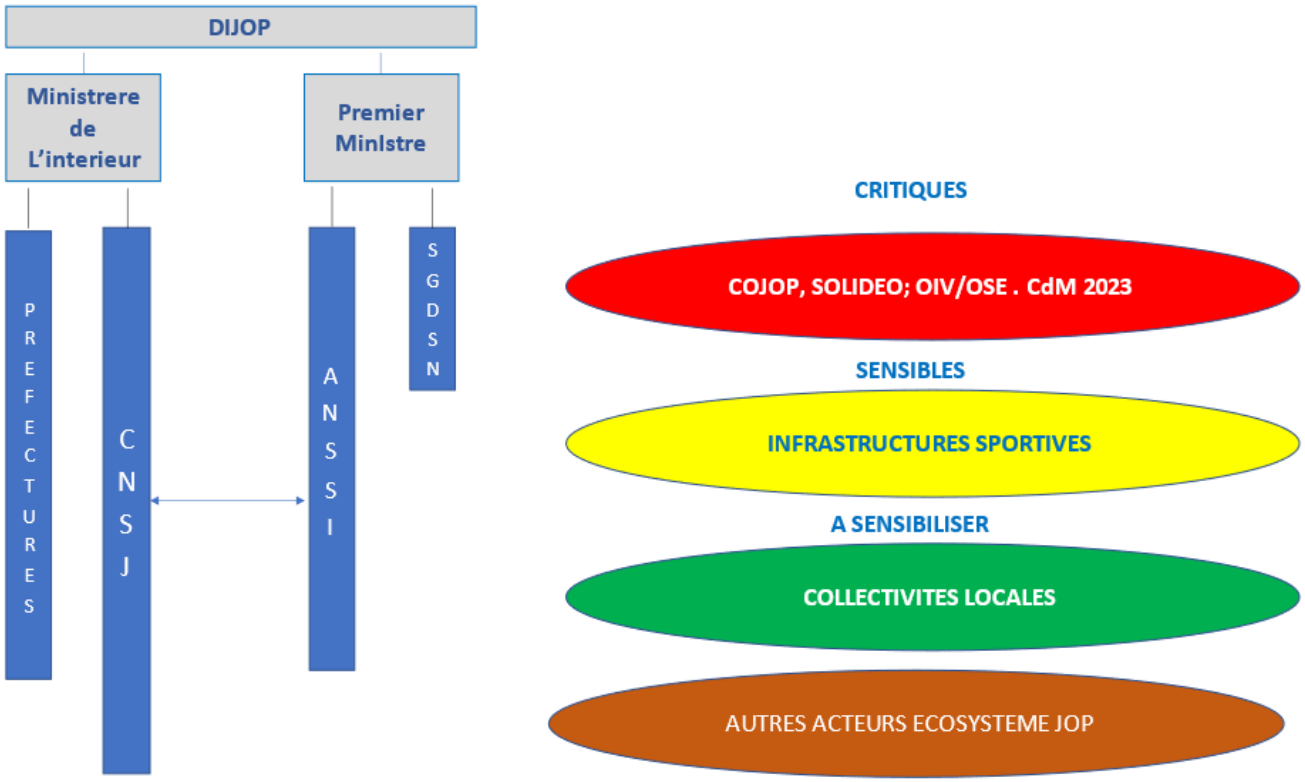
Il est cependant plus réaliste de prendre en compte les attaques avérées (attaques organisées ne relevant pas de bots, de scans automatisés aux cibles aléatoires …) qui se sont élevées à 70 000 lors des Jeux de Tokyo ce qui est 9 fois plus qu'aux Jeux de Londres.

ComCyberGend prévoit que par rapport à Tokyo 2020, les attaques soient fortement multipliées lors des Jeux de Paris 2024.

[5] *ATOS*
[6] *Secrétariat d'Etat du Royaume-Uni*
[7] *ATOS*

8. STRATEGIE DE CYBERSECURITE POUR LES JOP DE PARIS 2024

8.1. Stratégie de l'Etat : en cours de validation



Lors du Conseil olympique et paralympique du 25 juillet 2022, le Président de la République a désigné l'ANSSI pour piloter la stratégie de prévention des cyberattaques. Dans ce cadre, l'Agence procède à l'identification des entités de l'écosystème des JOP 2024 (qui sont souvent communes avec l'écosystème France 2023), environ 210 à ce jour, dont les collectivités territoriales-hôtes, pour leur proposer plusieurs services en fonction de leur niveau de criticité et de sensibilité afin d'assurer leur résilience (audit personnalisé ou automatique, assistances techniques, supervision, parcours de sécurité, sensibilisation…). La stratégie de l'ANSSI sera présentée aux autorités ministérielles concernées et au DIJOP au début du 4ème trimestre 2022.

8.2. Stratégie de la Collectivité-hôte à l'occasion des Jeux

S'agissant des collectivités hôtes, il leur appartient de s'assurer de mettre en place la bonne stratégie cybersécurité sur leur périmètre de responsabilité. A ce jour, aucune autre action particulière n'est donc formellement attendue d'elles à court terme du COJOP ou de l'Etat, si ce n'est d'être sensibilisées au sujet et aux risques auxquelles elles s'exposent. Il leur est notamment conseillé d'appliquer les standards et les recommandations de l'ANSSI et de Cybermalveillance.gouv.fr.

Il appartiendra donc à la collectivité locale de mettre en place sa stratégie cybersécurité à l'occasion des Jeux.

Elle devra :

- Mobiliser élus et direction des services à la cause Cybersécurité en tant que collectivité hôte à risque ;
- Attribuer les responsabilités au sein de la gouvernance, et instaurer un mode collaboratif, pour casser les silos et fonctionner en « cybersécurité by design » ;
- Procéder à sa propre analyse de risque par processus, afin de pouvoir adapter ses dispositifs de sécurité ;
- Cartographier les systèmes d'information, les données sensibles, les classer par zone de criticité, et ensuite décliner des scenarios de défense stratégiques puis tactiques ;
- Mettre en place (en interne ou en externe) :
    - La bonne protection correspondante de ses systèmes ;
    - Un process de détection de menace, (il en existe plusieurs sur le marché), afin de pouvoir traiter en priorité les incidents et les vulnérabilités qui constituent le plus grand risque pour l'organisation.
- Prévoir un système de gestion de crise et de réponse aux événements.

L'analyse des risques se décline par processus (i.e. un ensemble d'activités), par exemple :

- Activités sportives (compétitions, entraînement) ;
- Activités non-sportives à caractère olympique (célébrations, fan zone) ;
- Accueil du public, accueil des délégations, centres d'entrainement, de préparation, gestion des ressources humaines travaillant sur l'événement, autres populations olympiques et paralympiques accréditées ; relais de la flamme, gestion des flux ;
- Activités non sportives : Transports…

Conséquences potentielles des cyberattaques pour les Collectivités :

- Préjudice d'image ;
- Pertes de données, vol de données personnelles ;
- L'arrêt des missions de service public entrainant :

  - Des préjudices pour les administrés et pertes de confiance ;
  - Des préjudices financiers directs (reconfiguration du système d'information) et indirects (Indisponibilité d'équipements publics comme la fermeture d'une piscine municipale, d'un musée, ou d'un parking public) ;
  - Des dommages aux personnes ou aux biens (ex. : accident du fait d'un dysfonctionnement affectant la signalisation ou l'éclairage public).
- Arrêt du système opérationnel entrainant des perturbations (caméras de surveillance, feux de circulations, écrans, …)

9. RECOMMANDATIONS AUX COLLECTIVITES HOTES

Il ne s'agit plus d'échapper à la cyber malveillance, mais de faire face à cette réalité incontournable et relever ce défi, qui constitue un enjeu politique majeur pour les collectivités locales.

Aussi, comme dans d'autres domaines, Paris 2024 représente une opportunité pour la collectivité hôte, de se mettre à l'état de l'art en matière de cybersécurité, au nom de l'héritage des Jeux.

L'approche doit être globale et collaborative

- Traiter la cybersécurité comme un problème transdisciplinaire, recouvrant à la fois, les systèmes, les matériels, les organisations et l'humain ;
- Elle doit passer par une sensibilisation au risque cyber des élus, des directions fonctionnelles, opérationnelles, et des utilisateurs, (le sujet n'est plus l'antivirus sur les PC, mais concerne les réseaux, les applications, les données, le cloud, les objets connectés...) ;
- Penser « secure by design » : tout projet lié à un grand événement doit inclure une dimension cybersécurité dès son origine, en ayant une approche systémique incluant tous les composantes (stades, transports, ressources informatiques, billetterie, sécurité, hospitalité).

Il conviendra de démarrer par une analyse de risque de la Collectivité, en cartographiant les éléments sous sa responsabilité en prise avec l'évènement, de près ou de loin. Pour ce faire, les premiers éléments possibles sont :

- L'enceinte sportive de la collectivité où se déroule l'événement, et notamment les éléments en place à l'année, et qui ne seront pas « apportés » par le COJOP ;
- Le système d'information et de communication de la collectivité territoriale ;
- Les transports, et les voix d'accès à l'enceinte ;
- Les zones de célébrations et zones culturelles ;
- Le dispositif d'hébergement ;
- La gestion des données personnelles des volontaires.

Actions possibles recommandées :

- Pour les élus démarrer le processus immunité Cyber (questionnaire pour sensibiliser les élus à la cybersécurité de Cybermalveillance.gouv.fr avec COMCYBERGEND).

- Sensibiliser les agents car le facteur humain est souvent la cause de négligences et d'un manque de vigilance permettant des cyberattaques. Il s'agira notamment de les sensibiliser aux bonnes pratiques concernant les mots de passe, la protection des comptes de type réseaux sociaux, la détection des pièges qui leurs sont tendus (hameçonnage), via la messagerie. Exemple monter des opérations anti-phishing
- Pensez également à sensibiliser les citoyens face à la menace de faux sites utilisant le thème des JOP, et pouvant se faire passer pour les services de la collectivité hôte, à des fins d'extorsion ou d'acquisition de données.
- Suivre les conseils émis dans les différentes publications sur le sujet émanant de l'ANSSI, la Banque des Territoires, la Gendarmerie Nationale, de Cybermalveillance.gouv.fr (voir plus loin dans la bibliographie).
- Apprendre à gérer une crise en amont et organiser des simulations impliquant tous les services, pour se mettre en situation d'attaque.
- S'assurer d'être au bon niveau (effacer la dette cyber), notamment en actualisant son parc technologique pour ensuite envisager les analyses de risque liées au JOP.
- Tester les capacités de défense de vos enceintes sportives sur des scénarios possibles tels que :

    - Brouillage des réseaux wifi ;
    - Mise hors services des caméras ;
    - Diffusion des messages anxiogènes ;
    - Prise de contrôle de la gestion technique et envoi de fausses informations de supervision ;
    - Alteration du système de paiement des parkings ;
    - Accès à la messagerie.

- En cas d'attaques :

    - La collectivité doit s'efforcer d'avoir la capacité de traiter l'incident (elle peut pour cela faire appel à un prestataire, ce qui est facilité si un contrat a été signé en amont) et contacter l'ANSSI. Il est souhaitable d'informer le COJOP si l'incident semble lié aux Jeux ;
    - Déposer plainte sans délai auprès des forces de l'ordre, guichet unique que ce soit au niveau de la Police ou de la Gendarmerie ;
    - ComCyberGend peut alors dépêcher sur place experts techniques, experts judiciaires et spécialiste de la gestion de crise.

Enfin dernière recommandation, il est totalement déconseillé de payer une rançon. Dans la réalité il s'avère en outre que dans 50% des cas vous ne recouvrez pas les données perdues.

Cela incite aussi d'autres attaquants à vous cibler.

De moins en moins d'assurances assurent le risque Cyber si l'assuré n'est pas suffisamment protégé.

10. RECOMMANDATIONS PRATIQUES

Le risque zéro en matière de cybersécurité n'existe pas. L'évolution du marché de la sécurité tend vers le zéro trust (zéro confiance par défaut).

Il s'agira en priorité d'être vigilant à la fois sur le contrôle d'accès aux réseaux informatiques, sur la protection des utilisateurs, des postes de travail, des données et des applications.

Voici donc un ensemble de recommandations à appliquer qui protégeront la collectivité et l'évènement, en les appliquant aux périmètres à risque.

✓ Superviser les accès externes et savoir détecter toute connexion suspecte

- Avoir un process et des outils de détection des menaces (appelés EDR : Endpoint Détection and Response, pour les terminaux, et XDR (Extended Detection Response) pour l'ensemble du système d'information. Des outils ou services qui détectent les programmes malicieux et déconnectent les systèmes infectes pour éviter la propagation, sont devenus indispensables.

- Encadrer le nomadisme :

  - Authentifiez les utilisateurs à partir de n'importe quel appareil, de n'importe quel endroit ;
  - Ne donner l'accès aux réseaux qu'à des ordinateurs protégés ;
  - Imposer un système d'authentification multi facteurs à distance (sur mobile par exemple), afin d'identifier les personnes autorisées à se connecter au réseau. En effet le mot de passe tout seul ne suffit pas pour protéger en ligne. Un second facteur d'authentification est donc incontournable pour résister aux cybermenaces ;
  - Utiliser un VPN (réseau privé virtuel) pour chiffrer les connexions extérieures et renforcer la sécurité des accès distants, en donnant l'accès qu'à des éléments authentifiés.

✓ Segmenter les droits d'accès aux réseaux en fonction du type d'utilisateur et de son habilitation (ce qui permettra de détecter des comportements anormaux)

✓ Faire l'inventaire de tous les éléments connectés au réseau

De la même manière que dans le cadre du RGPD il convient de faire l'inventaire des données personnelles présentes dans son système d'information, et d'en connaitre l'utilité dans le cadre des process existants, il est important de faire l'inventaire de tous les objets connectés à son réseau, pour mieux en connaitre la surface d'attaque.

Les routeurs, les commutateurs, les points d'accès et tout autre matériel permettant de se connecter au réseau, devront aussi faire partie de cet inventaire et rentrer dans le process de sécurisation et d'inventaire.

✓ **Avoir un process de veille des vulnérabilités et de mises à jour**

- Une fois que tous les éléments connectés à un réseau sont recensés, il est capital de s'assurer que toutes les mises à jour logicielles (correctifs) concernant chacun d'eux sont bien appliquées. Ceci est valable pour les PC, mais aussi pour les commutateurs, routeurs réseaux (qui eux-mêmes embarquent du logiciel), les objets connectés.
- L'objectif est de s'assurer notamment qu'ils ne présentent pas de vulnérabilités facilitant les attaques. (Ex : porte dérobée ou backdoor : accès tenu secret à l'utilisateur aux données contenues dans un logiciel ou du matériel).

✓ **Mettre en place des solutions empêchant les utilisateurs de visiter des domaines malveillants sur le WEB (inconsciemment ou non)**

✓ **Protéger vos bornes wifi, vos routeurs et commutateurs en les sécurisant et ainsi protéger les données des utilisateurs**

✓ **Mettre en place un système de sondes intelligent sur le réseau afin d'observer 24h/24 et détecter tout mouvement anormal et les cybermenaces.**

✓ **Avoir une politique de sauvegarde**

En cas d'attaque de type rançongiciel (ransomware), il est indispensable de pouvoir récupérer ses données au plus vite. Pour cela il est indispensable d'avoir un politique de sauvegarde, avec des back-ups réguliers, automatisés et externalisés.

✓ **Mettre en place un Centre d'Operations de Sécurité COS (ou SOC)**

Il peut être interne à la collectivité ou externalisé. Le doter d'une plateforme centrale d'analyse, de visualisation, de suivi des données et de détection des anomalies.

✓ **Abonnez-vous à des réseaux de renseignements sur les menaces cyber dans le monde**

Ils vous permettent d'anticiper la suite et d'adopter des renseignements partagés et exploitables. Lorsque vous êtes au courant de ce qui se passe au sein de votre réseau et dans le monde entier, vous pouvez plus facilement envisager ce qui peut arriver.

✓ **Organiser des tests d'intrusion**

✓ **Mettre en place un plan de continuité et de reprise d'activité pour la collectivité associée à l'évènement en cas de cyber attaque.**

Ils doivent couvrir 80% des systèmes critiques pour obtenir des bons résultats.

✓ **Exécutez plusieurs activités de récupération chaque mois, en évaluant et en testant diverses parties du plan.**

Rappelez-vous que les capacités de continuité et de récupération ne sont aussi fortes qu'elles sont exercées au préalable.

✓ **Protéger les données personnelles des volontaires bénévoles de la collectivité, conformément au Règlement Général sur la Protection des Données (RGPD)**

Pour les plus petites collectivités, les mesures les plus élémentaires recommandées par Cybermalveillance.gouv.fr sont :

- La sécurisation des postes de travail (antivirus, EDR, etc.) ;
- La sécurisation des éléments réseau (pare-feu, proxy, etc.) ;
- La mise à jour régulière et suivie des systèmes et logiciels utilisés ;
- La mise en place de sauvegardes régulières et régulièrement testées ;
- La mise en place d'un système d'authentification fiable et robuste des utilisateurs ;
- Le chiffrement des flux réseau à travers internet et des supports de stockage (notamment les ordinateurs portables et les clés USB) ;
- La définition d'une politique d'habilitation clairement définie pour limiter les accès aux données ;
- La mise en place de journaux de connexion et leur supervision afin de détecter une compromission.

11. BIBLIOGRAPHIE

- Guide : obligations et responsabilités des collectivités locales en matière de cybersécurité (cnil.fr) (cybermalveillance.gouv.fr)

https://www.cnil.fr/sites/default/files/atoms/files/cybermalveillance.gouv_.fr-cnil_guide_sur_les_obligations_et_responsabilites_des_collectivites.pdf

- Guide pratique pour une collectivité et un territoire numérique de confiance (Banque des territoires, 2020).

https://www.cybermalveillance.gouv.fr/medias/2020/10/Guide-collectivite-confiance.numerique.pdf

- Kit de sensibilisation (Cybermalveillance.gouv.fr, janvier 2020). https://www.cybermalveillance.gouv.fr/tous-nos-contenus/kit-de-sensibilisation

Liste des ressources mises à disposition par le dispositif Cybermalveillance.gouv.fr

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/liste-des-ressources-mises-a-disposition

- Anticiper et gérer sa communication de crise cyber

https://www.ssi.gouv.fr/administration/guide/anticiper-et-gerer-sa-communication-de-crise-cyber/

- Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique

https://www.ssi.gouv.fr/administration/guide/crise-dorigine-cyber-les-cles-dune-gestion-operationnelle-et-stratégique/

- Les 10 mesures essentielles pour assurer votre cybersécurité (cybermalveillance ;gouv.fr)
- Les 10 mesures essentielles pour assurer votre cybersécurité - Assistance aux victimes de cybermalveillance

Documents ANSSI

- Organiser un exercice de gestion de crise cyber | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Attaques par rançongiciels, tous concernés – Comment les anticiper et réagir en cas d'incident ? | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)
- Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation | Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

- Guide d'hygiène

https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/

- Guide journalisation des SI Microsoft en environnement Active Directory

https://www.ssi.gouv.fr/guide/recommandations-de-securite-pour-la-journalisation-des-systemes-microsoft-windows-en-environnement-active-directory/

- Guide d'administration sécurisée

https://www.ssi.gouv.fr/guide/securiser-ladministration-des-systemes-dinformation/

- Guide "Interconnexion d'un SI à Internet"

https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.2.pdf

- Guide nomadisme

https://www.ssi.gouv.fr/guide/recommandations-sur-le-nomadisme-numerique/

- Guide maîtrise des risques

https://www.ssi.gouv.fr/guide/maitrise-du-risque-numerique-latout-confiance/

12. REMERCIEMENTS

Remerciements à la DIJOP, à la CNSJ, l'ANSSI, le COJOP, le CRO, ComCyberGend, à la DCPJ, et à l'Université Bretagne Sud pour les entretiens, leur collaboration active et leurs éclairages.

Dans le cadre du programme de travail annuel 2022, ce document a été rédigé avec la collaboration de Cisco, notre partenaire infrastructures de cybersécurité, d'équipements réseaux et de logiciel de visioconférence avec le soutien de Keneo.

A propos de Cisco

Depuis près de 40 ans, Cisco se positionne en tant que leader des équipements réseaux. La plupart des comptes du CAC 40 font ainsi confiance à Cisco.

Actuellement, 80% du trafic Internet mondial passe par l'infrastructure Cisco

Sa connaissance du réseau l'a naturellement orienté vers la cybersécurité et l'automatisation de ses solutions.

Ainsi sur la Cybersécurité près de 300000 clients dans le monde lui font confiance, notamment pour sa capacité à proposer une gamme complète et ouverte, sur un marché très fragmenté.

Son architecture Cisco Secure protège déjà 840 000 réseaux, 67 millions de boîtes aux lettres et 87 millions de terminaux pour des clients du monde entier.

Cisco propose également son service de détection de menaces Talos, pour tirer parti d'une visibilité approfondie des menaces et prendre le pouls des cyber événements d'aujourd'hui. (Talos a été utilisé au Superbowl par exemple)

Cisco vient de lancer le nouveau service Talos Intelligence On-Demand, disponible dès maintenant, offrant des recherches personnalisées sur le paysage des menaces propres à chaque organisation et peut vous aider grâce à des recherches personnalisées et vous informer sur les risques et les menaces spécifiques.

A propos de Keneo

Keneo est une agence de marketing sportif fondée en 2008.
Structurée autour de 4 expertises métiers (Consulting, Event, Servicing et Brand experience), et d'un pôle créatif transversal, Keneo possède une profonde connaissance de l'écosystème sportif et des enceintes sportives qui permet d'apporter des solutions créatives et pragmatiques.
Keneo et ses 32 collaborateurs bénéficient d'une longue expérience dans l'organisation de grands événements sportifs, dans le conseil aux institutions, le servicing et l'activation de marques dans l'univers du sport. En 2022, elle investit dans un événement propriétaire issu du monde de la voile de compétition, le Pro Sailing Tour.

À l'avenir, l'agence compte :

- Capitaliser sur ses 4 expertises historiques ;
- Développer les stratégies événementielles et « Héritage » des collectivités ;
- Se développer en direction du sport-santé (pratique d'activités physiques dans les entreprises) et de l'e-sport.