École Hexagone

Mastère Cyberdéfense

La cybersécurité dans les infrastructures sportives modernes

Mémoire de fin d'études réalisé par **Antoine COCHARD**

Encadré par **Docteur Cyril-Alexandre PACHON**

Suivi par mon tuteur d'apprentissage **Alain VERDY**

Année universitaire 2024-2025

Résumé

La digitalisation a révolutionné la façon dont les infrastructures sportives fonctionnent et interagissent avec leurs membres et les spectateurs. Les infrastructures sportives cherchent à optimiser leurs processus internes en utilisant des technologies de pointe pour améliorer leur efficacité et leur compétitivité. Cependant, ce développement s'accompagne également de risques.

Les infrastructures sportives sont devenues des cibles d'intérêt pour les cybercriminels. Elles ont une visibilité mondiale, notamment pendant les matchs ou les grands événements. Elles possèdent également des ressources financières et des informations sensibles. Les enjeux sont divers. Cela peut être générer de l'argent, s'amuser, promouvoir une idéologie ou une politique, exfiltrer des données. Les attaques principales dans ce domaine sont les attaques par DDoS, les rançongiciels, le social engineering, les attaques sur les objets connectés, le vol et l'exfiltration de données sensibles, ainsi que les attaques web.

Face à ces risques cyber, les infrastructures sportives cherchent à se protéger. Elles mettent en place des mesures de sécurité, des formations et des actions de sensibilisation auprès du personnel. Elles déploient des solutions techniques telles que la gestion des privilèges d'accès, l'authentification multifacteur, la segmentation des réseaux, le chiffrement des données, les EDR et les pare-feux. Ces mesures permettent de protéger les infrastructures contre les tentatives d'intrusion, qu'elles soient virtuelles ou physiques.

Ces mesures de sécurité ont notamment été mises en place pour la sécurisation des Jeux Olympiques 2024. Malgré un nombre de cyberattaques plus élevé qu'aux Jeux Olympiques de Tokyo en 2020, ceux de Paris en 2024 n'ont pas été perturbés. La coordination des différents acteurs de la cybersécurité, la mise en place de procédures et de mesures techniques ont permis aux JO 2024 de se dérouler sans accroc. C'est une première historique comparée aux événements précédents. Les JO 2024 sont un exemple à suivre pour l'organisation de grands événements sportifs.

Sommaire

Table des matières

Liste des figures et tableaux

Glossaire

Terme	Définition
ANSSI	Agence nationale de la sécurité des systèmes d'information.
AMA	Agence Mondiale Antidopage.
APT	Advanced Persistent Threat est une cyberattaque prolongée et ciblée.
ASM	Association Sportive Montferrandaise.
AWS	Amazon Web Services est une plateforme de cloud.
Botnet	Groupe d'ordinateurs ou de dispositifs sous le contrôle d'un attaquant, utilisé pour mener des activités malveillantes contre une victime ciblée.
CISA	Certified Information Systems Auditor est une certification qui témoigne de l'expertise d'un professionnel capable de réaliser des audits, de contrôler et de surveiller les technologies et systèmes informatiques d'une entreprise.
CNIL	Commission Nationale de l'Informatique et des Libertés.
DDOS	Distributed Denial of Service.
ENISA	Agence de l'Union européenne pour la cybersécurité.
EBIOS RM	Besoins et Identification des Objectifs de Sécurité, Risk Manager.
IA	Intelligence Artificielle

IDS	Intrusion Detection Systems.
INSEP	Institut National du Sport, de l'Expertise et de la Performance.
IOT	Internet of Things.
IPS	Intrusion Prevention Systems
ISO	International Organization for Standardization.
JO	Jeux Olympiques.
PCA	Plan de continuité d'activité.
PRA	Plan de reprise d'activité.
Rançongiciel	Logiciel malveillant ou virus qui bloque l'accès à l'ordinateur ou à ses fichiers et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès.
RGPD	Règlement général sur la protection des données.
SQL	Structured Query Language est un langage de programmation le plus courant utilisé dans les bases de données relationnelles.
TLS	Protocole utilisé par les applications pour communiquer de manière sécurisée à travers un réseau.
VAR	Video Assistant Referee est une technologie vidéo qui ajoute plus de précision aux décisions de l'arbitre.
VLAN	Virtual Local Area Network est un réseau LAN virtuel et indépendant.

WAF	Web Application Firewall protège le serveur d'applications Web dans le backend des multiples attaques (phishing, rançongiciel, attaque DDOS, malware).
WIFI	Wireless Fidelity est une technologie de mise en réseau sans fil qui permet aux appareils électroniques de se connecter de manière transparente à un réseau via des fréquences radio.
XSS	Le cross-site scripting est une attaque informatique sur les sites web qui voit les cybercriminels exécuter des scripts malveillants sur des sites Web légitimes ou de confiance.
Zero-day	Attaque qui tire parti d'une vulnérabilité de sécurité pour laquelle aucun correctif n'a été mis en place

Préface

Ce mémoire de fin d'études clôture mon parcours universitaire en sécurité informatique. Il a été rédigé dans le cadre de mon Mastère Cyberdéfense à l'École Hexagone de Clermont-Ferrand.

C'est lors de ma dernière année de lycée que j'ai choisi de m'intéresser de plus près à l'informatique. J'ai été fasciné par l'étendue des possibilités et par la pluralité des sujets, et j'ai décidé d'effectuer mes études supérieures dans ce domaine. Je suis progressivement devenu passionné par l'informatique, et plus particulièrement par la sécurité de celle-ci. Depuis, j'ai toujours cherché à apprendre les nouvelles technologies. En 2023, j'ai obtenu mon diplôme de licence professionnelle des métiers réseaux informatiques et télécommunications. Cette formation, certifiée par l'Agence nationale de la sécurité des systèmes d'information m'a permis de rejoindre le mastère cyberdéfense à l'École Hexagone. Ce mastère me permet d'élargir mes connaissances générales et d'approfondir les points techniques de sécurité.

Au cours de mon apprentissage au sein du Groupe Titel, j'ai eu l'occasion d'explorer les domaines de la sécurité des réseaux et des systèmes, tant dans un contexte administratif qu'industriel. Étant amené à administrer des équipements et à développer des procédures liées à ce thème, j'ai souhaité m'y intéresser en détail afin d'approfondir mes connaissances théoriques. Passionné de sport et pratiquant à haut niveau, j'ai naturellement choisi de m'orienter vers ce milieu pour mon mémoire, combinant ainsi mes intérêts personnels et professionnels. Ma curiosité initiale pour ce sujet, marqué par des enjeux émergents et souvent méconnus, s'est rapidement transformée en un intérêt profond. Cela m'a conduit à choisir ce thème pour mon mémoire. Celui-ci s'articule autour des spécificités d'une organisation dans le milieu du sport, puis en présentant les différentes menaces potentielles dans ce milieu, et les solutions techniques qui répondent aux nouvelles méthodes d'attaques, notamment lors des Jeux Olympiques 2024.

Remerciements

Je tiens à exprimer ma profonde gratitude à toutes les personnes qui m'ont apporté leur aide et leur soutien durant la rédaction de ce mémoire de fin d'études.

Tout d'abord, j'adresse mes remerciements les plus sincères à mon tuteur d'apprentissage, Monsieur Alain VERDY, responsable du Service Informatique au sein du Groupe TITEL, pour sa disponibilité et ses conseils réguliers tout au long de ma réflexion.

Je souhaite aussi exprimer ma gratitude envers trois autres collègues de mon équipe, Madame Marion NURY, responsable de la hotline CRM, Madame Khaoula FARHANI, chargée de projet en système d'information, et Monsieur Benjamin VALET, chef de projet informatique. Merci pour leurs aides précieuses, les informations apportées et leur temps pour répondre à chacune de mes questions.

Ensuite, je tiens à remercier sincèrement Madame Christelle COCHARD et Monsieur Yann COCHARD pour leur relecture attentive et leurs retours pertinents, qui m'ont permis d'avoir un avis externe éclairé sur mon travail et d'améliorer considérablement la qualité de ce mémoire.

Enfin, je voudrais exprimer toute ma reconnaissance envers mon directeur de mémoire, Docteur Cyril-Alexandre PACHON, pour m'avoir permis d'acquérir les outils nécessaires à la rédaction de ce mémoire. Je lui suis très reconnaissant, ainsi qu'à tout le personnel de l'École Hexagone, pour m'avoir apporté cette opportunité de développer mes compétences professionnelles au cours de ce projet.

Introduction

Depuis les années 1990, les infrastructures sportives modernes se développent. Les grands stades emblématiques, les centres d'entraînement spécialisés, les académies sportives réputées comme la Rafa Nadal Academy et des organisations de renom telles que l'INSEP deviennent des organisations importantes. Derrière ce monde sportif, les technologies du numérique sont de plus en plus utilisées. La digitalisation touche désormais tous les aspects de la gestion et de la performance dans le sport. Les technologies numériques permettent d'optimiser l'organisation et l'administration des événements sportifs. Cela permet d'analyser les performances en temps réel, de mieux comprendre les besoins des athlètes et d'améliorer les conditions d'entraînement par des outils connectés. Cependant, cette transformation s'accompagne également de risques. Les infrastructures sportives connectées sont devenues des cibles d'intérêt pour les cybercriminels. Les infrastructures sportives ont une visibilité mondiale, notamment pendant les matchs ou gros événements. Elles possèdent également des ressources financières et des informations sensibles. Les enjeux sont divers. Cela peut être faire de l'argent, s'amuser, promouvoir une idéologie/politique, exfiltrer des données.

La cybersécurité dans le secteur sportif est aujourd'hui un enjeu stratégique. La cybersécurité est plus qu'importante, notamment pour les événements internationaux de grande envergure comme les coupes du monde de rugby, le tournoi de tennis de Roland-Garros, ou encore les Jeux olympiques de Paris 2024. Ces événements attirent des millions de spectateurs et de passionnés dans le monde entier, tout en mobilisant des infrastructures informatiques de grande taille. Lors de ces événements, les infrastructures sportives deviennent les cibles de cyberattaques. Un incident de sécurité peut causer des perturbations majeures, allant de la désorganisation des compétitions à la perte de données sensibles des athlètes ou des spectateurs. En raison de ces enjeux, les organisateurs doivent redoubler d'efforts pour anticiper les menaces et mettre en place des mesures de protection adaptées. Le but est de garantir le bon déroulement des événements, de préserver la réputation du secteur sportif à l'échelle internationale et de garantir le chiffre d'affaires.

Les cyberattaques qui visent le secteur sportif sont variées et deviennent de plus en plus sophistiquées. Parmi les types d'attaques les plus fréquentes, les attaques par déni de service distribué (DDoS), qui visent à paralyser les services en ligne des infrastructures sportives. Mais aussi les attaques par rançongiciels, qui bloquent l'accès aux systèmes jusqu'au paiement d'une rançon. L'hameçonnage (phishing) est également

courant et permet aux attaquants d'obtenir des informations confidentielles en usurpant des identités. Les infrastructures sportives de plus en plus connectées sont également exposées aux attaques ciblant les objets connectés, qui constituent des points d'accès potentiellement vulnérables aux réseaux. En 2023, il y a eu une hausse de 30 % des attaques par rançongiciels dans le monde du sport, et cette tendance met en évidence l'ampleur de la menace. Ces attaques mettent en danger la confidentialité des données des athlètes, ainsi que la gestion de l'événement lui-même. Elles sont souvent le fait de groupes cybercriminels organisés, parfois même soutenus par des États, et exploitent des failles techniques ou des erreurs de configuration pour pénétrer dans les systèmes sportifs.

La sécurité des infrastructures sportives va bien au-delà de la simple protection des systèmes informatiques. Elle doit également couvrir la sécurisation des réseaux, la protection des données personnelles et stratégiques, ainsi que la sécurité physique des installations. Les organisations sportives doivent investir dans la formation continue du personnel. Cela va permettre de sensibiliser aux bonnes pratiques en matière de cybersécurité et de les rendre capables d'identifier des comportements suspects. Une intrusion, qu'elle soit virtuelle ou physique, peut avoir des conséquences graves. Une attaque peut porter atteinte à la réputation des organisations sportives si elle pénètre les systèmes d'information. Cela peut notamment nuire à la crédibilité de la structure et à leur relation avec le public. En ce qui concerne les infrastructures critiques comme les stades nationaux ou les centres d'entraînement d'élite, une cyberattaque pourrait entraîner des pertes financières, opérationnelles, et même humaines.

Les récents exemples d'attaques dans le secteur sportif montrent l'ampleur des conséquences que peuvent engendrer les incidents de cybersécurité. Lors de grands événements comme les Jeux olympiques, les cyberattaques sont fréquentes et peuvent prendre diverses formes. L'interrogation centrale de ce mémoire sera : Comment les infrastructures sportives peuvent-elles se protéger contre les cyberattaques, compte tenu de leur forte dépendance aux technologies numériques ?

I. Organisation informatique des infrastructures sportives

1. Les infrastructures sportives modernes et leurs équipements

1.1. Les grands stades et centres sportifs

Les infrastructures sportives modernes, les grands stades, les centres d'entrainements, les associations sportives utilisent tous les nouvelles technologies émergentes. Ces technologies ont pour but d'améliorer l'expérience des athlètes, des spectateurs, des salariés et des adhérents d'une association. Cependant, cette digitalisation n'a pas que des avantages. Les infrastructures s'exposent à des risques de sécurité informatique.

Les stades modernes sont constitués de centaines d'appareils connectés. Ce n'est plus seulement des lieux de compétition sportive. Ce sont des « mini-entreprises » avec une infrastructure informatique propre. Par exemple, le court Philippe-Chatrier à Roland-Garros a intégré très récemment un toit rétractable, des équipements d'analyse vidéo, de la diffusion en direct en 4K ainsi qu'un système de VAR, aussi appelé « Hawk-Eye ». Toutes ces innovations permettent d'améliorer l'expérience des sportifs et des spectateurs, et elles sont connectées.

Lors des Jeux Olympiques et Paralympiques, la plupart des stades ont utilisés de nombreuses technologies. Il y a eu notamment des réseaux Wi-Fi publics, des systèmes d'analyse des foules en temps réel. Le rapport du CERT-FR 2024 mentionne le fait que ce genre d'infrastructures est conçu pour être capable de gérer des flux massifs de données tout en garantissant une bonne sécurité face aux cyberattaques. (ANSSI, Panorama de la cybermenace 2023, 2023)

Des institutions comme l'INSEP, Institut National du Sport, de l'Expertise et de la Performance, possèdent les centres d'entrainements en France avec la plus grande qualité. Ils possèdent une qualité matérielle, professionnelle mais aussi technologique. L'INSEP possède des équipements sportifs très récents. Ce genre d'équipements sportifs est connecté. Cela va permettre d'obtenir des données. Des capteurs, des systèmes de suivi biométrique et des outils sont utilisés par les athlètes pour effectuer des analyses vidéo. Cela donne aux entraîneurs la possibilité de créer des programmes sportifs et alimentaires personnalisés pour chaque athlète. (PAULS, 2023)

Les clubs sportifs, tels que ASM Rugby et Clermont Foot, bénéficient également des avancées technologiques pour améliorer leurs performances et l'engagement des supporters.

J'ai notamment eu l'opportunité d'avoir un échange en visioconférence avec le Directeur des Systèmes d'Information du Clermont-Foot. Cet échange m'a permis de poser à M. GERARD-DEPALLE plusieurs questions sur les infrastructures des clubs sportifs, des données, de la gestion informatique, de la sécurité informatique. Il m'a notamment fait la comparaison suivante, « *Un club sportif, c'est comme un parc d'attraction. Nous vendons des billets à l'avance avec un nombre de places bien précis. Nous faisons consommer les visiteurs (buvettes, restaurant). Nous faisons consommer les visiteurs à la boutique officielle du Clermont-Foot. Et enfin, nous faisons passer un bon moment à tout le monde* ». Le Clermont-Foot est composé d'une soixantaine de salariés, moitié dédiés à la partie administrative, et moitié à la partie sportive.

Les infrastructures sportives modernes offrent de grandes opportunités, mais elles font face à des défis en cybersécurité. Selon le rapport du CERT-FR 2024, les attaques peuvent cibler des systèmes critiques. Cela inclut la billetterie, la gestion des flux vidéo ou les bases de données des sportifs. La numérisation accrue expose à des risques comme le vol de données, les rançongiciels ou les sabotages électroniques. Cependant, des mesures adaptées permettent de protéger ces infrastructures tout en exploitant leur potentiel technologique.

Selon le "Cahier 1 : Cadre, enjeux et objectifs de la digitalisation des enceintes sportives", la digitalisation vise plusieurs objectifs. Elle cherche à améliorer l'expérience des usagers, optimiser la gestion des infrastructures et valoriser les données collectées. Cependant, cette transformation numérique exige une attention particulière à la cybersécurité. Cela permet de prévenir les risques liés à la connectivité accrue des systèmes.

1.2. Les équipements connectés pour les athlètes (capteurs, IoT, wearables)

Les équipements connectés permettent d'améliorer la performance, la préparation physique, et aussi d'assurer un suivi de l'état de santé. Cette technologie est rapidement devenue indispensable dans le sport professionnel.

Les infrastructures modernes utilisent plusieurs équipements connectés différents. Les écrans géants et les panneaux LED permettent de retransmettre l'événement sportif en direct ainsi que des statistiques (temps de possession, le score pour le football, le nombre d'aces et le score pour le tennis). Les LED placées en bord de terrain tout autour permettent d'afficher les sponsors, des publicités et aussi d'interagir avec les spectateurs.

La sécurité et la gestion des infrastructures sont gérées par des systèmes de contrôle d'accès et de caméras pour la vidéosurveillance. Il est aussi possible d'utiliser des solutions biométriques ou des badges RFID afin de garantir que les personnes puissent accéder à des zones réservées. Les applications mobiles permettent de simplifier l'expérience utilisateur pour l'achat de billets et la localisation de leurs places.

Les technologies vidéo et les drones sont également présents dans l'ensemble des stades et infrastructures. Le Clermont-Foot a dû mettre en place avec le prestataire de la ligue 28 caméras tout autour du stade uniquement pour la retransmission vidéo. Ces caméras sont utilisées pour filmer au mieux les athlètes afin d'offrir des moments en direct à la télévision.

Les objets connectés utilisés dans le sport, tels que les patchs de suivi GPS et les capteurs de santé, permettent de collecter des données corporelles et physiques. Ces dispositifs surveillent en temps réel des paramètres comme la fréquence cardiaque, l'oxygénation et la fatigue, et transmettent les informations aux équipes techniques lors des matchs. Après les compétitions, ces données sont analysées par des prestataires. Dans les centres d'entraînement comme l'INSEP, des équipements connectés, tels que des tapis de course, chaussures connectées et montres intelligentes, permettent également de récolter des données pour ajuster les sessions d'entraînement. Le concept du "quantified self", ou automesure, est devenu incontournable pour analyser les performances. La surveillance en temps réel joue un rôle clé dans la prévention des blessures en permettant d'ajuster l'intensité des séances dès les premiers signes de fatigue ou de surmenage. (Ministère des sports, s.d.)

1.3. Les technologies pour les spectateurs : Wi-Fi, applications mobiles, streaming

Les technologies mises en œuvre pour les spectateurs dans les équipements sportifs sont importantes pour qu'ils aient une bonne expérience lors des matchs. Le Wi-

Fi permet d'avoir une bonne connexion grâce aux points d'accès qui sont placés à des emplacements stratégiques du stade. Les applications pour smartphones permettent aux utilisateurs d'acquérir des tickets, de réserver des repas et des boissons, tout en suivant les informations importantes du match en direct.

La diffusion en direct nécessite une bande passante élevée afin de n'avoir aucune coupure. Le but est d'avoir un streaming ininterrompu, ce qui est essentiel, surtout lors de grands événements. Cependant, ce genre de technologie présente également des contraintes. Il faut faire attention à la gestion du flux de données afin que la bande passante ne soit pas saturée. Il est important de protéger les données que les utilisateurs transmettent via l'application ou bien lors de la connexion au Wi-Fi.

Au sein de l'infrastructure du Clermont-Foot, il y a 120 antennes Wi-Fi. Sur chaque antenne Wi-Fi sont diffusées 2 SSID. Chaque SSID est associé à un VLAN distinct. Il y a un SSID public et un SSID privé. Pour ce qui est de la retransmission vidéo via les 28 caméras dans le stade, il y a une fibre dédiée. Les flux vidéo et les flux informatiques sont isolés physiquement. Le débit de la bande passante est alloué par le pare-feu. Il y a plusieurs arrivées Internet (SFR, Orange, FREE). Cela permet d'assurer une continuité de service lors des grands événements sportifs. (iTech, 2024)

2. Technologies utilisées dans le sport

2.1. Systèmes d'arbitrage vidéo et drones

L'arbitrage vidéo est de plus en plus répandu dans le monde du sport. Les arbitres que ce soit dans le football, le rugby, le tennis, le badminton utilisent de plus en plus la VAR. Cela permet à l'arbitre d'avoir des décisions plus précises, mais aussi d'afficher d'autres informations aux spectateurs. L'IFAB, l'International Football Association Board, a indiqué que l'arbitre assistant vidéo examine systématiquement les séquences vidéo pour chaque action décisive. Lorsqu'il y a un but, un penalty ou un carton rouge, il est capable de conseiller l'arbitre principal via un microphone afin de revoir la décision. Des entreprises spécialisées ont développé des solutions pour faciliter l'implémentation de la VAR. Par exemple, VOGO propose VOGOSPORT ELITE, une solution d'arbitrage vidéo certifiée par la FIFA, qui permet une diffusion en direct et en replay des actions de jeu, offrant ainsi aux arbitres un outil performant pour analyser les situations litigieuses.

Les drones permettent d'offrir de nouveaux angles de vue. Ils parviennent à se déplacer rapidement et capturent des images aériennes à une vitesse pouvant atteindre

70km/h. Les drones ont été utilisés lors des Jeux Olympiques de 2024 pour une épreuve de kitesurf. Cela permettait aux jurés d'avoir une vue d'ensemble de la course. Cependant, il est nécessaire de prendre des précautions quant à l'utilisation des drones. Les accidents liés à la chute de drones sur des spectateurs sont problématiques. La fédération québécoise des sports cyclistes rappelle que l'utilisation d'un drone est interdite au-dessus du parcours et à moins de 10 mètres de celui-ci. (Gouv, s.d.)

2.2. Plateforme de billetterie et de gestion des spectateurs

Les infrastructures sportives modernes qui proposent des matchs avec du public (comme le club du Clermont-Foot, les matchs de l'ASM ou bien Rolland-Garros) utilisent toutes des systèmes de billetterie. Les plateformes de billetterie permettent aux spectateurs d'acheter des billets via des sites web ou des applications mobiles. Les solutions utilisées sont souvent Eventbrite, Weezevent, Yurplan. Ce sont des solutions qui permettent de gérer les billets, les tribunes et les ventes. (Cyberdéfense, 2024)

La gestion des spectateurs est maintenant effectuée par des systèmes intelligents qui se basent sur l'intelligence artificielle. Ces systèmes intelligents analysent en temps réel les foules au sein des stades et des tribunes. Ils permettent d'étudier le mouvement des foules et sont très utilisés lors de la fin de match ou en cas d'incendie. L'entreprise Avigilon propose des solutions de vidéosurveillance, contrôle d'accès et d'analyse basées sur l'intelligence artificielle.

3. Exigences spécifiques de sécurité des données dans le sport

3.1. Typologies des données sensibles

Les infrastructures sportives modernes possèdent de nombreuses données. La CNIL, Commission nationale de l'informatique et des libertés, explique que les données sensibles sont une catégorie particulière des données personnelles. L'article 2 de la loi informatique et libertés précise qu'une donnée à caractère personnel est une « information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ». (Légifrance, s.d.). Il est important de pouvoir protéger les données confidentielles. Il est essentiel de respecter le principe de la CIA, « Confidentiality, Integrity, Availability ». (Fortinet, s.d.)

La figure 1 montre les différents types de données à caractère personnel. Il y a différentes informations telles que l'identité, les coordonnées, la vie personnelle, la vie professionnelle, les informations économiques et financières, les données de connexions, les données de localisation. Ce sont souvent des données qui peuvent être accessibles sur internet via l'OSINT (Open Source Intelligence). Ce type de données est accessible sur les réseaux sociaux, sur les pages jaunes, sur LinkedIn, sur des factures, sur des billets de matchs.

Les données d'identification sont des données sensibles, telles que les informations de santé, biométriques, les opinions politiques, les origines ethniques et le casier judiciaire. Ces informations sont protégées et conservées par des hôpitaux, des organismes, des mairies, les forces de l'ordre.

Et enfin, les données à caractère personnel qui sont perçues comme sensibles regroupent les numéros de sécurité sociale, les photos et vidéos, les données bancaires. En février 2024, la CNIL a estimé que plus de 33 millions de personnes ont vu leurs informations de sécurité sociale fuiter. Une attaque a eu lieu sur Viamedis et Almerys. Ce sont deux opérateurs qui assurent la gestion du tiers payant des complémentaires santé. Les données concernées des assurés et de leur famille sont, l'état civil, la date de naissance et le numéro de sécurité sociale, le nom de l'assureur santé ainsi que les garanties du contrat souscrit. (HARRINGTON, 2023)

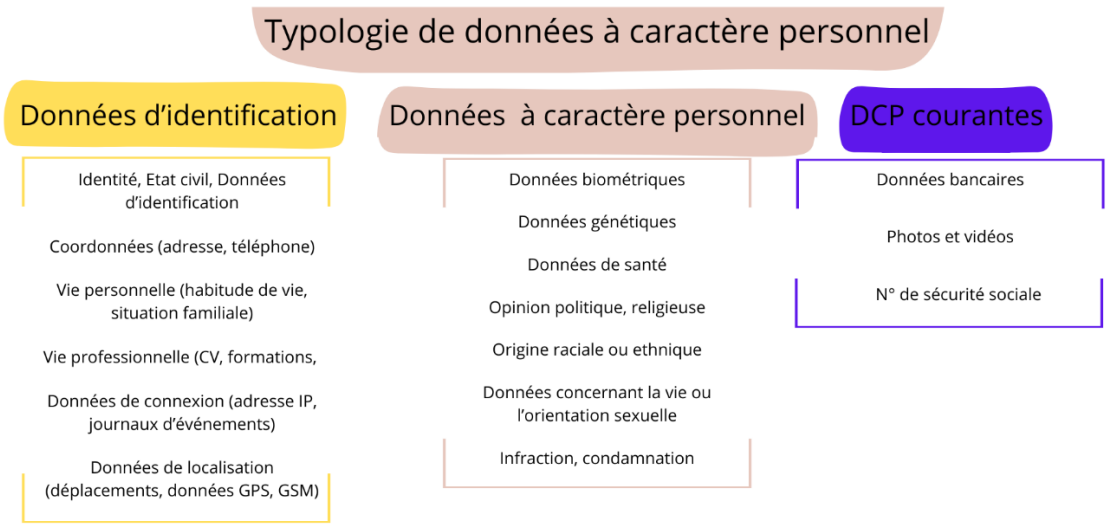

Figure 1, Typologie de données à caractère personnel (DCP)

Les données financières sont constituées de contrats, de sponsoring, des revenus de la billetterie, des buvettes, des restaurants, des boutiques, ou encore les salaires des sportifs. Ces données sont souvent la cible des cybercriminels.

Les données médicales regroupent les diagnostics, traitements, résultats d'examens et historiques médicaux. Elles sont sensibles et protégées par des cadres juridiques stricts. La divulgation de ces informations pourrait entrainer des atteintes à la vie privée ou être exploitée de manière inappropriée.

Les données stratégiques sont par exemple, les plans tactiques, les analyses de performances ou les stratégies de recrutement. Ce sont également des informations confidentielles. L'exposition de ce genre d'informations pourrait donner un avantage aux équipes adverses ou bien compromettre certains projets.

Et enfin, les données opérationnelles sont les données de la logistique des événements sportifs. Il y aura les plannings, les plans de sécurité, les déplacements professionnels. Ce genre d'informations n'est pas critique, mais il permet le bon déroulement des matchs ainsi que la sécurité des athlètes et des spectateurs. (School, s.d.)

3.2. Régulations légales et normes

Les données sensibles RGPD sont des données à caractère personnel qui, si elles sont révélées ou si elles font l'objet d'un traitement, sont susceptibles de mener à des discriminations. Cette catégorie de données personnelles est soumise à des règles juridiques particulières. Le RGPD en interdit la collecte et le traitement sauf « exceptions limitatives ». Les traitements temporaires (conservation temporaire, enregistrement ou encore collecte) font l'objet de la même interdiction. Selon l'article 9 du RGPD, (RGPD, s.d.) les informations concernées par les limitations de traitement des données dites sensibles sont l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques ou données biométriques aux fins d'identifier une personne physique de manière unique, les données concernant la santé (notamment le numéro de sécurité sociale), les données relatives à la vie sexuelle ou l'orientation sexuelle. Il est possible de collecter les informations des athlètes, des salariés, des spectateurs, ainsi que toute autre personne sous certaines conditions. L'article 9.2 du RGPD énonce les conditions de cette collecte.

Lorsque la personne a donné son consentement explicite pour une ou plusieurs finalités spécifiques. Cette condition ne s'applique que si le consentement de la personne concernée est libre, spécifique et informé. Lorsque les informations recueillies ont été rendues publiques par la personne concernée. Lorsque le traitement des données sensibles RGPD s'avère nécessaire à la sauvegarde de la vie de la personne. Si cette collecte et le traitement sont nécessaires à l'exécution des obligations en matière de droit du travail, droit social ou à la constatation, l'exercice ou à la défense d'un droit en justice. Si ces données se révèlent nécessaires à la gestion des membres d'un organisme à but non lucratif tel qu'un syndicat, un parti politique ou encore une association religieuse ou philosophique. Lorsque ces données sont reconnues nécessaires pour des motifs d'intérêt public (santé publique), des fins d'archives pour la recherche scientifique ou historique et des fins de statistiques (sous réserve de garanties).

Le traitement des données sensibles RGPD est strictement réglementé. Le RGPD exige ainsi un principe de licéité et un principe de minimisation des données. L'article 6 du RGPD explique les 6 conditions pour lesquelles le traitement des données par les entreprises est licite. « La personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ». « Le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ». « Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ». « Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ». « Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ». « Le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ». Le traitement est indispensable aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que les intérêts ou les droits fondamentaux de la personne concernée, en particulier lorsqu'il s'agit d'un enfant, ne prévalent et exigent une protection des données personnelles. Ce dernier point ne s'applique pas au traitement effectué par les autorités publiques dans le cadre de leurs missions. (CNIL, CHAPITRE II - Principes, s.d.)

Le RGPD contraint les entreprises à réduire les risques liés au traitement des données sensibles, notamment en termes de cybersécurité. Le règlement européen énonce trois principes, le principe de confidentialité, le principe d'intégrité et le principe de disponibilité (CIA). Pour réduire les risques d'atteinte à la sécurité, le règlement européen suggère également les mesures de sécurité telles que le chiffrement, la pseudonymisation, les antivirus, les mots de passe robustes, les mesures physiques ou matérielles telles que le verrouillage des portes, les mesures organisationnelles (procédures, gouvernance).

Les personnes dont les données ont été collectées ont des droits sur leurs données privées. Il s'agit du droit d'accès, qui permet de savoir si une entreprise ou un organisme traite leurs données personnelles, d'en obtenir la communication et de contrôler leur exactitude ; du droit de rectification ; du droit à l'effacement (ou droit à l'oubli), du droit à la limitation du traitement ; de l'obligation notification en cas d'effacement, de rectification ou de limitation du traitement ; du droit à la portabilité de leurs données ; du droit d'opposition.

La norme ISO/IEC 27001 est une norme de système de management de la sécurité de l'information (SMSI). Elle définit les exigences auxquelles un système de management de la sécurité de l'information doit répondre. Cette norme fournit aux entreprises des lignes directrices pour l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue d'un système de management de la sécurité de l'information. La conformité à ISO/IEC 27001 signifie qu'une organisation ou une entreprise a mis en place un système pour gérer les risques liés à la sécurité de ses données ou des données qu'elle est amenée à traiter, et que ce système est conforme aux bonnes pratiques et principes énoncés dans cette Norme internationale. Le DSI du Clermont-Foot choisit principalement ses prestataires informatiques, que ce soit pour les logiciels et applicatifs, service support (Ressources humaines, Informatique, Commerce, Marketing), ou bien le suivi des performances, suivi des autres clubs, de la billetterie, externalisation des données, des sauvegardes qui possèdent la norme ISO27001. (CNIL, Guide de la sécurité des données personnelles, 2024)

3.3. Enjeux liés à la confidentialité et à l'intégrité des données

Les entreprises font face à trois grands types d'enjeux. Tout d'abord il y a des enjeux organisationnels. Pour pouvoir respecter les droits des citoyens européens (comme l'accès, la rectification, le droit à l'oubli, la limitation, la portabilité, l'opposition,

etc.), les entreprises doivent attribuer des ressources pour tout ce qui va être lié à la manipulation de données. Les organisations sont tenues de nommer un délégué à la protection des données si elles font partie du secteur public ou si elles surveillent fréquemment un grand nombre de personnes, ou encore si leurs opérations nécessitent le traitement de données sensibles ou liées à des crimes ou condamnations judiciaires à grande échelle.

Il y a aussi les enjeux de développement et d'image de marque. Le RGPD offre aux entreprises une chance de gagner la confiance de leurs clients et patients. En suivant le principe de mise à jour et de correction des informations concernant leurs clients (tels que les fichiers de facturation et les prospects), les entreprises optimiseront leur performance commerciale et augmenteront leur productivité.

Selon le MEDEF, « La sauvegarde des données personnelles est une stratégie pour l'entreprise afin d'accroître la confiance qu'elle entretient avec ses clients, ses associés et ses employés, dans un environnement de plus en plus digital ».

Et enfin, il y a des enjeux d'ordre financiers et judiciaires. Des amendes administratives définies par les autorités de contrôle sont encourues en cas de non-respect des dispositions du RGPD. Ces dernières peuvent atteindre 10 millions d'euros ou représenter 2 % du chiffre d'affaires global du groupe à l'échelle mondiale. Pour les infractions plus sévères, les entreprises peuvent obtenir des amendes jusqu'à 20 millions d'euros ou 4 % de leur chiffre d'affaires mondial.

4. Particularités des infrastructures sportives comparées à d'autres secteurs

4.1. Comparaison avec les secteurs bancaires, industriels et militaire

Dans le secteur bancaire, les enjeux de la cybersécurité sont multiples. Le premier va être de protéger les données sensibles des clients, les données personnelles ainsi que les données financières. Si les hackers ont accès à ces informations, ils pourront effectuer des virements frauduleux, usurper l'identité des clients de la banque ou encore revendre leurs données personnelles. Le deuxième enjeu est de limiter les conséquences financières lors d'une cyberattaque. Les institutions financières doivent être en mesure d'anticiper et de neutraliser les cyberattaques qui les visent. Si elles échouent et que l'attaquant arrive à ses fins, ils doivent considérer la cyber-résilience pour minimiser les pertes et sauvegarder le capital ainsi que les clients. Et enfin, ils doivent préserver la réputation de la banque. Les clients qui décident de placer leur argent dans une

institution financière, ou de contracter un prêt et une assurance auprès de cette dernière, doivent être en mesure d'accorder leur confiance à l'établissement en question. Une banque proposant une sécurité de premier ordre est susceptible d'attirer un plus grand nombre de clients.

En décembre 2024, une attaque de cheval de Troie a eu lieu dans plusieurs banques françaises. Le malware « DroidBot » a ciblé la banque Axa, la banque Populaire, le BNP Paribas, Boursorama, la Caisse d'Épargne, le CIC, le Crédit Agricole, le Crédit mutuel Arkéa, LCL et la Société Générale. Le malware se faisait passer pour une application populaire. Il combinait des fonctionnalités classiques de VNC caché et de superposition avec des fonctionnalités souvent associées aux logiciels espions. Il comprend un enregistreur de frappe et des routines de surveillance qui permettent l'interception des interactions des utilisateurs, ce qui en fait un outil puissant de surveillance et de vol d'informations d'identification.”

Le secteur industriel est confronté à des menaces différentes. Les enjeux de la cybersécurité dans les systèmes industriels vont être la négligence humaine, les vulnérabilités dans les systèmes d’information industriels. Les négligences humaines font partie des risques de cybersécurité. Elles peuvent créer des vulnérabilités qui peuvent ensuite être exploité par les attaquants. Il est important de former le personnel et de les informer sur les enjeux. (ANSSI, La cybersécurité des systèmes industriels, s.d.)

Les réseaux industriels comportent de nombreuses vulnérabilités. Ils sont principalement constitués d’automates, d’imprimantes de production et de serveur SCADA. Ces systèmes sont souvent pauvres en mécanismes de sécurité et peuvent être exploités par des attaquants motivés et organisés. D’autre part, les éditeurs de logiciel du monde industriel n’effectuent pas autant de mises à jour et de patchs de sécurité que dans les réseaux administratifs, de par ses contraintes de disponibilité et de sûreté. La figure 2 montre les impacts potentiels sur les systèmes.

Dommages matériels / corporels	La modification des configurations nominales des installations peut provoquer des dégradations physiques avec le plus souvent des conséquences matérielles – mais parfois aussi humaines.
Perte de chiffre d'affaires	L'interruption de la production génère des manques à gagner importants. La modification de paramètres de fabrication conduisant à des produits non conformes génère des coûts importants.
Impact sur l'environnement	La défaillance du système suite à une prise de contrôle malveillante peut générer un dysfonctionnement des installations (ouverture de vannes de produits polluants) et provoquer une pollution du site et de son environnement. Un tel incident s'est produit en Australie ces dernières années.
Vol de données	Perte de secret de fabrication, contrefaçons, avantage pour la concurrence.
Responsabilité civile / pénale - Image et notoriété	L'indisponibilité du service comme la rupture de distribution d'électricité ou d'eau, ainsi que la fourniture de produits défectueux mettant en danger le consommateur peuvent aboutir à des poursuites pour les dommages occasionnés ou simplement dégrader l'image de l'entreprise (la satisfaction du client et sa confiance).

Figure 2, Impacts potentiels sur les systèmes industriels

(ANSSI, La cybersécurité des systèmes industriels, s.d.)

Dans le domaine militaire, la cybersécurité est une priorité stratégique. Le but va être de pouvoir faire face aux cybermenaces. Les cyberattaques peuvent déséquilibrer l'intégralité de la souveraineté nationale. La cybersécurité dans l'Armée est dirigée par le Ministère des Armées et plus particulièrement par le COMCYBER. Les missions du COMCYBER vont être de protéger le Ministère, les données confidentielles, d'assurer la sécurité des forces armées dans le cadre de leurs opérations, la prévention de la cyberguerre, mais aussi la résilience face à ce nouveau danger et enfin l'affirmation de la France en tant que cyber puissance à l'échelle mondiale. Les missions de l'Armée en cybersécurité sont à la fois défensives et offensives. Il s'agit en premier lieu d'organiser la cyberdéfense du pays et en second lieu de mener des opérations cybermilitaires. Elle sert à la fois d'élément dissuasif, d'élément défensif, et d'outil de cyber-surveillance.

4.2. Les défis spécifiques liés à la nature publiques des événements sportifs

Les infrastructures sportives partagent certains défis de ces secteurs, notamment la protection des données sensibles (personnelles, financières et médicales). Cependant, ce qui est vraiment caractéristique des infrastructures sportives, c'est la disponibilité lors des événements. Il y a une forte exposition sur les réseaux sociaux, les télévisions et il n'est pas possible d'avoir une coupure avec des milliers voire des millions de

téléspectateurs. Au sein du club de Clermont-Foot, il y a beaucoup d'externalisation de services sous contrats avec des prestataires. Les prestataires s'occupent des logiciels, de l'applicatif, du service support, du stockage des données de performances, de santé, des données personnelles, de la billetterie, des caméras. L'infrastructure réseau est segmentée par des VLANs. Les flux vidéos, les flux informatiques, les IoT, le Wifi, les écrans LEDs sont tous isolés physiquement par différentes fibres qui sont reliés jusqu'aux pare-feux. Le DSI a mis énormément d'importance sur le fait d'isoler les différents systèmes et d'allouer différentes fibres physiques pour chaque système afin d'assurer un maximum de disponibilité en cas d'incident.

II. Les attaques fréquentes dans le monde du sport

1. Attaques par déni de service distribué (DDoS)

1.1. Mécanismes d'attaques DDoS

Une attaque par déni de service (DoS) vise à saturer les ressources d'un système. Il ne sera plus capable de répondre à des demandes de services légitimes. Une attaque DDoS, aussi connue sous le nom d'attaque par déni de service distribué, vise également à vider les ressources d'un système. Une attaque DDoS se produit lorsque de nombreuses machines hôtes sont contaminées par des logiciels malveillants (botnets) et manipulées par l'attaquant. Ce sont les attaques « par déni de service » car le site ou la ressource ciblée par l'attaque ne peut pas assurer son service à ceux qui cherchent à s'y connecter. Une telle attaque produit du trafic de rétrodiffusion (backscatter), l'assaillant substitue son adresse par une adresse IP aléatoire avant d'expédier les paquets à la cible. Ainsi, le service se trouve submergé par une multitude de requêtes d'utilisateurs (celles produites par les pirates s'ajoutant aux demandes légitimes des utilisateurs du service) et devient hors service.

A noter qu'une attaque DoS peut être lancée depuis une seule machine, tandis qu'une attaque par déni de service distribuée (DDoS) provient de plusieurs périphériques qui génèrent simultanément un trafic gigantesque. Toujours dans le but de perturber l'accès à un service.

La figure 3 montre le fonctionnement d'une attaque par déni de service distribué. Un attaquant ayant pris possession de plusieurs machines hôtes. Il envoie énormément de trafic sur le serveur ciblé. L'attaquant envoie quatre gigabits de données par seconde alors que le serveur ne peut recevoir qu'un gigabit de données par seconde. Le serveur va être complètement saturé par toutes les requêtes qu'il reçoit.

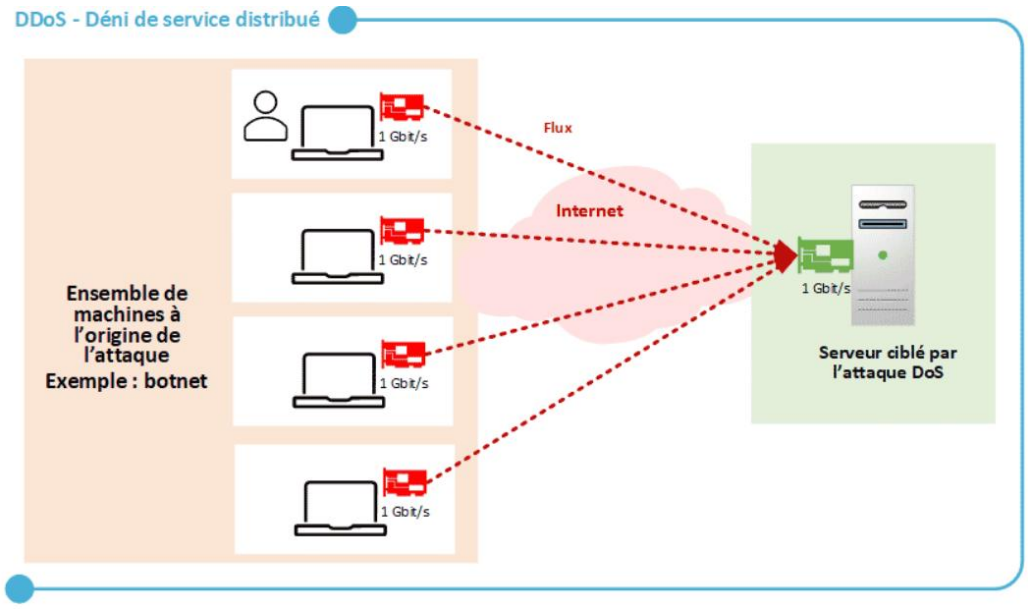

Figure 3, Attaque DDoS - Déni de service distribué

(BURNEL, 2022)

Au-delà du simple fait de bloquer l'accès à un service, l'objectif caché derrière cette attaque peut être motivé par plusieurs facteurs. Le premier est le financier, exiger une somme d'argent pour faire cesser ces cyberattaques. Le deuxième est la concurrence, un concurrent qui retransmet un match sportif afin de rediriger les téléspectateurs sur une autre chaine de télévision ou streaming. Pour terminer, les motivations peuvent aussi être d'ordre politique. C'est le « hacktivisme ».

Il y a plusieurs types d'attaques DDoS possibles. (ANSSI, NP_Guide_DDoS, s.d.) La première est les attaques par réflexion tireront parti d'ordinateurs accessibles sur le web qui répondent à des requêtes, en faisant usage de l'adresse IP falsifiée de la victime. L'agresseur transmet des paquets aux réflecteurs en exploitant l'adresse IP de la victime comme source. Les réflecteurs répondent à la cible, produisant un flux de trafic non désiré qui peut engorger les connexions réseau. Ces attaques ont souvent recours à des protocoles basés sur UDP, qui autorise la falsification d'adresse IP sans l'obligation de créer auparavant une session. Cela peut engorger les serveurs DNS ou applicatifs employés pour les diffusions vidéo ou les sites de vente de billets. L'attaquant interroge des serveurs DNS en usurpant l'adresse IP d'une plateforme de billetterie en ligne. Les réponses des serveurs surchargent la bande passante de la cible.

Les attaques par amplification exploitent des protocoles générant des réponses d'une taille très supérieure à celle des requêtes, maximisant ainsi le trafic généré. En combinant la réflexion et l'amplification, l'attaquant génère un trafic volumétrique capable de saturer la bande passante réseau ou les ressources de traitement de la cible. Il est possible d'exploiter des protocoles SSDP ou CHARGEN, sur des réseaux Wi-Fi publics pour inonder le débit des bornes Wi-Fi présentes dans un stade.

Les attaques volumétriques ont pour objectif d'épuiser la bande passante réseau disponible pour rendre des services indisponibles. En envoyant un volume massif de trafic (requêtes UDP, HTTP, ou TCP), l'attaquant va pouvoir perturber les services de billetterie ou de gestion des abonnés.

Les attaques ciblant les applications visent les faiblesses des applications, notamment en épuisant les ressources de traitement des serveurs. Le but va être de saturer les capacités des serveurs. L'attaque HTTP Flood envoie des milliers de requêtes HTTP (GET ou POST) pour épuiser les ressources des serveurs web des événements sportifs.

1.2. Olympic Destroyer à Pyeongchang

Une cyberattaque a eu lieu lors de la cérémonie d'ouverture des Jeux de Pyeongchang en 2018. C'est devenu la cyberattaque la plus marquante de l'histoire cyber des Jeux Olympiques. Je vais vous présenter comment l'attaque s'est déroulée, quelles en ont été les conséquences et à qui l'attaque a été attribuée.

La cérémonie d'ouverture a eu lieu le 9 février 2018, la cérémonie des Jeux Olympiques est diffusée en direct, et visualisée par des millions de téléspectateurs. C'est un événement très médiatisé. C'est lors de cet événement qu'a eu lieu la phase finale de la cyberattaque. Cette attaque a commencé quelques mois auparavant avec des phases de reconnaissance, d'infections, de propagations. L'attaque a commencé entre novembre 2017 et février 2018. Il était important pour les attaquants de bien se préparer en avance afin d'avoir suffisamment de temps pour se latéraliser, comprendre le réseau et identifier les actifs les plus critiques de l'infrastructure. La cyberattaque a débuté par une campagne d'hameçonnage. Les parties prenantes (les prestataires) ont reçu des mails avec des liens piégés. Les cyberattaquants ont essayé de se faire passer pour le Comité International Olympique, le Centre National du Contre-Terrorisme coréen ou encore le président-directeur général de l'entreprise prestataire responsable du chronométrage

des Jeux Olympiques. Au final, une entreprise prestataire du réseau informatique des Jeux a été compromise pendant le mois de novembre 2017.

Le maliciel, l'Olympic Destroyer s'est latéralisé de réseau en réseau. Il est programmé pour se propager automatiquement de réseau en réseau en exploitant la chaine d'approvisionnement. Le maliciel exfiltre les identifiants, les garde en mémoire, puis se réplique et se latéralise sur d'autres réseaux en utilisant les identifiants et les mots de passe collectés sur le système d'information. (Diaries, EP 77 : Olympic Destroyer, 2020)

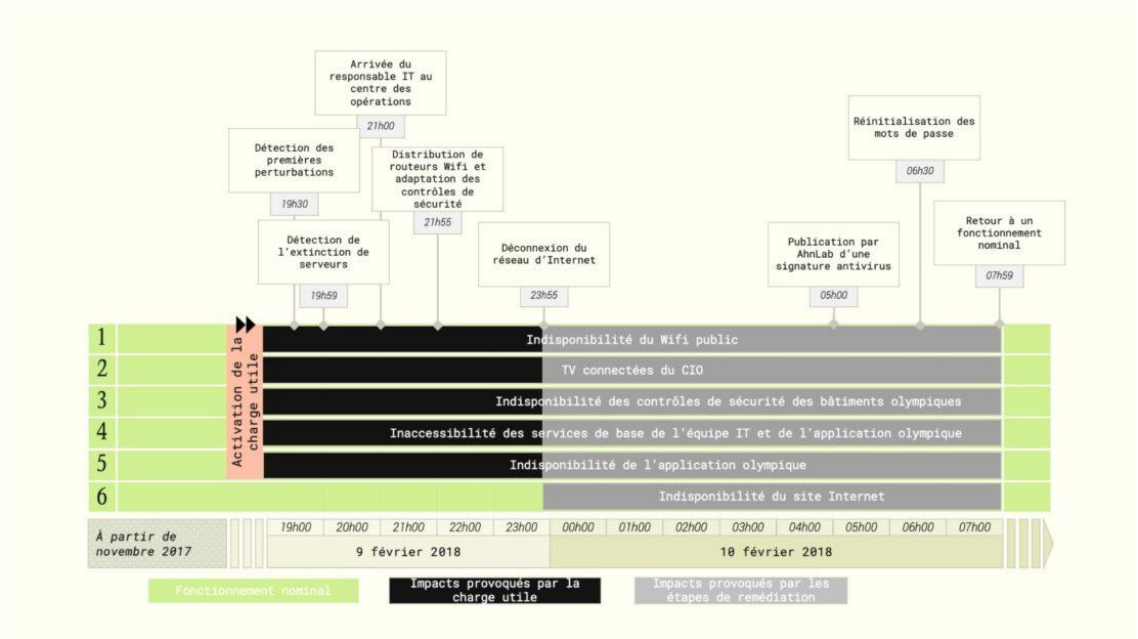

Figure 4, Chronologie de l'incident Olympic Destroyer entre le 9 et le 10 février 2018

(CTI-TEAM, 2024)

La figure 4 montre les différents incidents répertoriés par ordre chronologique lorsque les cyberattaquants ont activé l'Olympic Destroyer. L'activation a permis au maliciel de supprimer les paramètres de configuration d'initialisation des machines compromises, empêchant ainsi leur réinitialisation, puis à forcer l'arrêt du système d'information compromis. Les équipes de sécurité ont pu relever des signes de perturbations. Les bornes Wi-Fi, l'accès à l'application pour imprimer les tickets ainsi que les portails de sécurité RFID des Jeux Olympiques n'étaient plus disponibles. L'équipe technique du comité d'organisateur a rapidement entrepris des travaux de remédiation. Elle a mis hors ligne tout le système d'information de minuit jusqu'à 8h du matin pour pouvoir cloisonner les réseaux et identifier la menace. Cette opération s'est

bien passée, le système d'information a été rétabli en utilisant les sauvegardes faites au préalable. Cela a permis d'assurer la cérémonie d'ouverture ainsi que la suite des Jeux.

Suite à cette attaque, une étape d'investigation et de forensic a eu lieu pour comprendre le déroulement de l'attaque et découvrir l'auteur de cette même attaque. L'attribution d'une cyberattaque est un processus délicat. L'investigation pour déterminer l'auteur de l'Olympic Destroyer s'est achevée en 2020, 2 ans après l'incident. L'attribution nécessite plusieurs preuves irréfutables. Il faut à la fois des preuves techniques, mais aussi des preuves contextuelles. Cette investigation comporte des risques géopolitiques, si cette attaque est attribuée à un pays innocent, le pays peut se voir discrédité.

Le code derrière l'Olympic Destroyer a été conçu pour orienter le travail d'investigation vers de fausses pistes. C'est « le faux drapeau ». C'est une technique grâce à laquelle l'attaquant cherche à se faire passer pour quelqu'un d'autre. Le but est de conduire les défenseurs à ignorer ou à mal interpréter des artefacts ainsi que des éléments de preuves. Des chercheurs en sécurité informatique ont d'abord établi des liens techniques avec des maliciels déployés par des MOA présumés nord-coréen et chinois. L'éditeur de sécurité Cisco Talos a aussi rapporté avoir observé des fonctionnalités similaires avec BadRabbit et NotPetya, deux logiciels de sabotage qui partage des parties de code identiques avec l'Olympic Destroyer. Ensuite, l'éditeur de sécurité Kaspersky a attribué cette tentative de faux drapeau à Sandworm, d'origine russe. Selon cette source, l'objectif des attaquants était de perturber la cérémonie d'ouverture des Jeux Olympiques qui est un des événements les plus médiatisés.

Les Jeux Olympiques de Pyeongchang ont été marqués par les sanctions émises par le Comité International Olympique contre la Russie. La Russie a été accusée de tricherie lors des Jeux Olympiques d'hiver de Sotchi en 2014. Cette accusation a empêché les athlètes russes de participer sous leur drapeau, ils ont dû le faire sous bannière neutre. L'hymne de la Russie n'a pas été joué et le pays a dû payer une amende de 15 millions de dollars. En plus de ces sanctions, les chercheurs en sécurité informatique ont remarqué que les cyberattaques russes s'étaient intensifiées depuis 2015. Celle-ci est motivée par l'annexion de la Crimée en 2014 et la guerre de position contre l'Ukraine toujours en cours en 2018. Ces événements militaires ont généré des tensions avec les pays occidentaux, qui ont sanctionné économiquement la Russie.

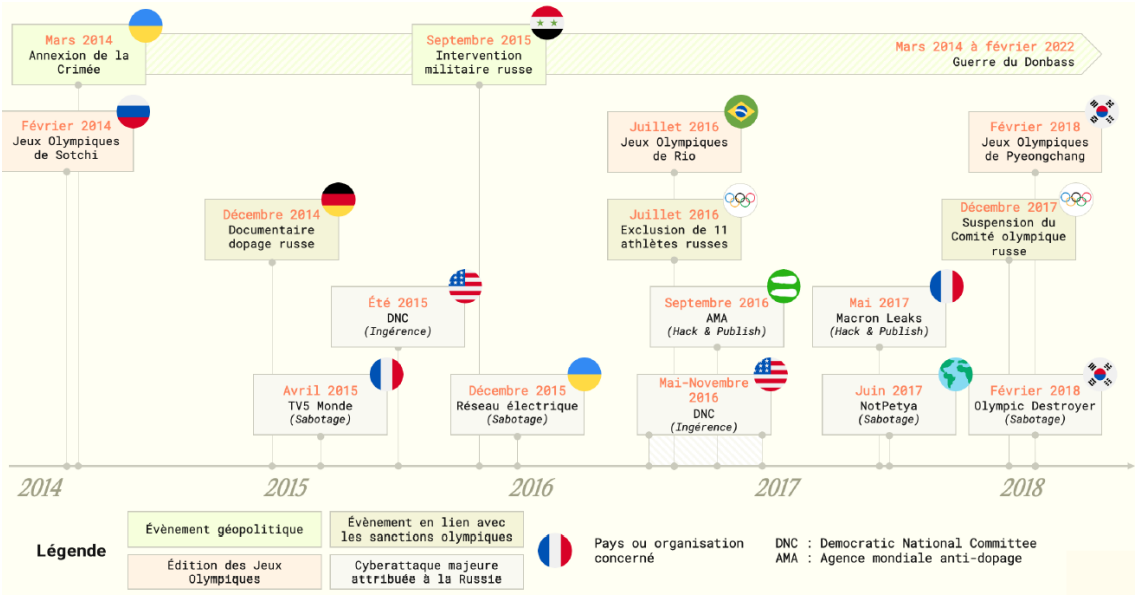

Figure 5, Chronologie des opérations offensives cyber attribuées à la Russie

Les conséquences de cette attaque n'ont pas eu de gros impacts sur la cérémonie d'ouverture. Cependant, cette attaque a interrompu les services en ligne. Les systèmes de billetterie ont été paralysés, empêchant les spectateurs de récupérer leurs billets électroniques. Les réseaux Wi-Fi du stade ont été désactivés, rendant impossible l'accès aux outils de communication pour les équipes techniques services en ligne. Ces interruptions ont eu un impact direct sur la réputation des organisateurs. L'image des Jeux Olympiques de Pyeongchang a été ternie par cet incident, renforçant la perception que les infrastructures numériques sportives ne sont pas suffisamment sécurisées face aux menaces modernes. L'attaque de Pyeongchang a marqué les personnes. Cela a permis de prendre la cybersécurité dans le sport plus au sérieux. Cette attaque a mis en évidence la nécessité de stratégies de défense renforcées pour protéger les infrastructures numériques et garantir la continuité des événements. (BARRAT, 2024)

2. Rançongiciels

2.1. Fonctionnement des rançongiciels

Un rançongiciel est une catégorie de logiciels malveillants. Le but des rançongiciels est de chiffrer les données d'un système, d'en restreindre l'accès afin de pouvoir extorquer une rançon à la victime. L'attaque suit généralement un cycle structuré, dont l'ANSSI en explique les étapes dans l'état de la menace rançongiciel. (ANSSI, Attaques par rançongiciels, tous concernés, 2020).

L'infection d'un système cible repose sur plusieurs méthodes. Les campagnes de phishing sont très fréquemment utilisées. L'attaquant envoie des e-mails avec des pièces jointes ou des liens malveillants aux victimes. Une fois ouverts, ils déclenchent l'exécution de rançongiciels. Les attaquants exploitent aussi des failles dans les systèmes, comme des vulnérabilités connues non corrigées ou des failles « Zero-Day ».

Le RDP (Remote Desktop Protocol) compromise est une autre méthode. Les pirates utilisent des failles, des erreurs de configuration ou des identifiants volés pour accéder illégalement à une machine via le protocole RDP. Ce dernier, utilisé pour gérer les systèmes Windows à distance, est une cible de choix.

Les scripts malveillants injectés dans des sites web, via des attaques « Cross-site Scripting », permettent d'infecter les navigateurs. Enfin, les attaques physiques complètent ces techniques. Elles incluent l'utilisation de clés USB infectées, de périphériques compromis ou encore le vol de badges et l'interception directe.

La figure 6 illustre notamment les principaux vecteurs d'attaques pour effectuer une attaque par rançongiciels. Les statistiques sont incomplètes et dépendent des compétences pour localiser les sources. Les accès RDP compromis sont populaires car revendus à bas prix sur les marchés illicites. L'hameçonnage domine, ciblant les attaques « Big Game Hunting ». Les entreprises appliquent mieux les mises à jour que les particuliers, mais leurs employés restent vulnérables aux e-mails trompeurs dans un contexte professionnel.

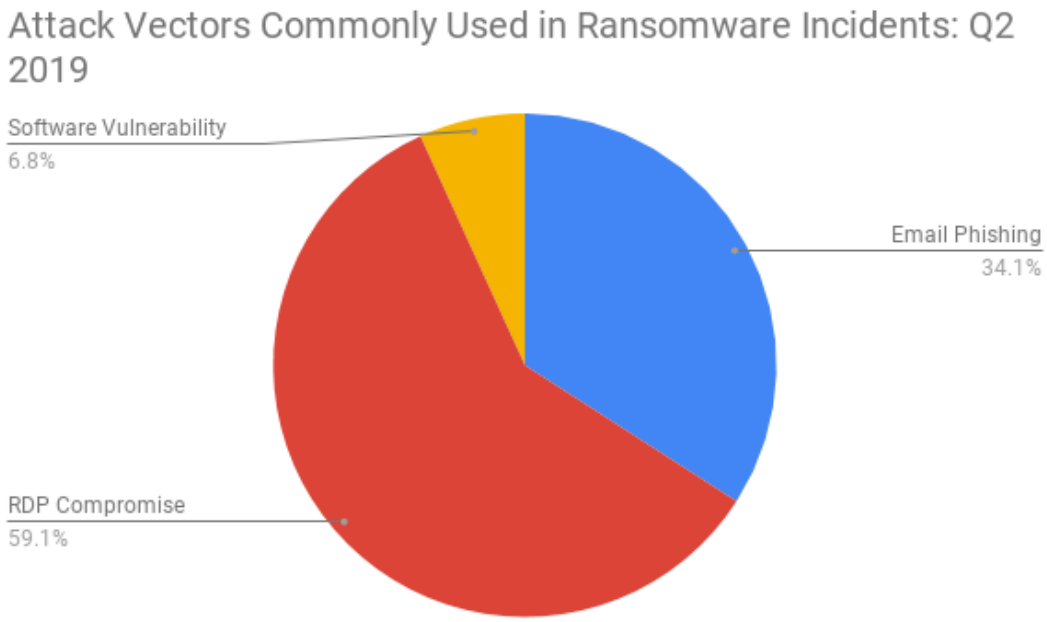

Figure 6, Vecteurs d'attaques utilisés pour délivrer des rançongiciels

(SIEGEL, 2019)

La deuxième étape est le processus de reconnaissance et de propagation. Une fois que l'attaquant a compromis une machine, les attaquants commencent une phase d'exploration du réseau pour identifier les cibles potentielles et essayer de compromettre d'autres machines.

Dans un premier temps, les attaquants mènent des reconnaissances pour collecter des informations sur l'infrastructure cible. Ils cherchent à identifier les services en ligne, les machines connectées, les privilèges des comptes utilisateurs et les vulnérabilités exploitables. Des outils courants comme Mimikatz, BloodHound, WireShark ou PowerShell Empire sont utilisés pour extraire des informations sensibles telles que des mots de passe ou des hachages. Ces données sont obtenues depuis la mémoire vive, les bases de données locales ou en écoutant le trafic réseau. Elles permettent aux attaquants de s'authentifier ou d'escalader leurs privilèges sur le réseau. En parallèle, ils surveillent les partages réseau, les bases de données accessibles, les serveurs critiques et les solutions de sauvegarde. Leur priorité est de cibler les ressources les plus stratégiques.

L'étape de propagation commence une fois les informations collectées. Les attaquants déploient des mécanismes de déplacement latéral pour infecter d'autres

machines et augmenter l'impact de l'attaque. Ils détournent souvent des protocoles et outils légitimes présents dans l'environnement, comme SMB (Server Message Block) pour accéder aux partages réseau, ou RDP pour établir des connexions à distance. Ces techniques permettent de minimiser les traces et d'éviter la détection par les systèmes de sécurité. Dans certains cas, des logiciels malveillants supplémentaires, comme des trojans, sont utilisés pour automatiser la propagation. Les attaquants exploitent aussi des vulnérabilités non corrigées, telles qu'EternalBlue pour Windows, afin de contourner les défenses.

Une fois une présence significative établie dans l'infrastructure, les attaquants adaptent leur stratégie à leurs objectifs. Si les attaquants souhaitent complètement stopper le système d'information de la victime, ils vont viser les systèmes critiques. Cela inclut les serveurs de fichiers, les bases de données et les solutions de sauvegarde. Pour atteindre cet objectif, ils déploient des scripts personnalisés. Ces scripts orchestrent le chiffrement simultané des données sur toutes les machines accessibles. Ils désactivent aussi les solutions de sécurité et suppriment les sauvegardes locales. Parfois, ils exfiltrent également des données sensibles.

La phase suivante est le chiffrement des données. C'est l'étape clé d'une attaque par rançongiciel. Le but est de rendre les fichiers inaccessibles pour les propriétaires légitimes. Les attaquants utilisent des algorithmes comme AES ou RSA pour verrouiller les données et garantir qu'ils détiennent la seule clé de déchiffrement. Les sauvegardes sont la cible prioritaire des attaquants. Le but est de rendre illisibles les sauvegardes de la victime afin qu'elle ne puisse pas restaurer le système d'information. Une fois les sauvegardes vérolées, ils vont se concentrer sur l'extorsion des fichiers critiques, des bases de données, des médias, des documents de productions.

L'étape ultime est la demande de rançon. Les attaquants exploitent la détresse des victimes pour les inciter à payer une rançon. Ils vont laisser un message, une note de rançon, expliquant toutes les étapes pour effectuer le paiement, généralement en cryptomonnaie pour préserver leur anonymat.

Les attaquants vont instaurer un climat de pression avec des délais stricts, augmentant parfois la rançon ou menaçant de détruire les données si la victime ne paie pas à temps.

La figure 7 présente notamment le nombre de paiements effectués suite au rançongiciel.

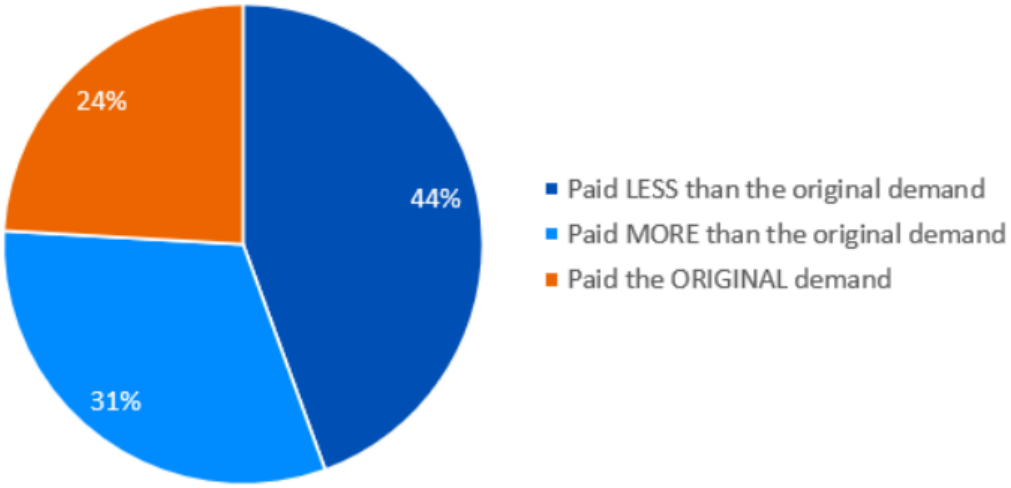

Figure 7, Pourcentage des paiements de rançons effectués.

(Adam, 2024)

Je vais vous présenter un exemple d'attaque dans le milieu sportif avec un club de football Italien qui n'a pas payé la rançon.

2.2. Attaque de rançongiciel sur le Bologna Football Club

Le Bologna Football Club 1909 a été victime d'une attaque. Le groupe de rançongiciel RansomHub a réussi à infiltrer le système d'information du club. Ils ont ensuite fait fuiter des données sensibles. RansomHub est un groupe de rançongiciel opérant selon le modèle du Ransomware-as-a-Service (RaaS). Les attaques attribuées à RansomHub se caractérisent par une approche méthodique, incluant l'exfiltration de données sensibles suivie d'une demande de rançon, avec la menace de divulguer les informations en cas de non-paiement.

En novembre 2024, le groupe RansomHub a réussi à infiltrer les systèmes d'information du Bologna FC. Les détails de l'intrusion n'ont pas été divulgués. Les sources les plus probables sont une campagne de phishing, des vulnérabilités logicielles et des identifiants avec des mots de passe faibles. Les attaquants ont ensuite déployé le rançongiciel sur le système d'information.

RansomHub

bolognafc.it

UPDATE!!!

The club's management refused to protect the confidential data of players and sponsors. Therefore in 2 days we will publish all medical, personal and confidential data of all players of the club. But we remind them that they will be able to get much more money through lawsuits than for playing in a club that betrayed them.

Bologna FC was hacked due to lack of security on their network. All confidential data has been stolen.

Bologna FC is violating GDPR laws and disclosing all internal club documents.

About:
Via Casteldebole 10, 40132 Bologna, Italy.
+39 051 611 1111.
comunicazione@bolognafc.it
bolognafc.it

Bologna FC does not have any data protection and its network which is why absolutely all their data was stolen.

All sponsorship contracts and documents disclosing the amounts and conditions of all sponsors were stolen
All financial data of the club for the whole period of its existence was stolen.
Stolen all personal and confidential data of the players
All documents revealing transfer strategies including new players and young

Figure 8, Message du groupe RansomHub sur le darkweb

La figure 8 illustre le message du groupe RansomHub sur le darkweb. Le groupe RansomHub a demandé une rançon auprès de la direction du club, celle-ci n'a pas été payée. « La direction du club a refusé de protéger les données confidentielles des joueurs et des sponsors ». « Par conséquent, dans deux jours, nous publierons toutes les données médicales, personnelles et confidentielles de tous les joueurs du club ». Le groupe RansomHub a mis en vente les données sur le darkweb. Le gang du rançongiciel affirme que les données divulguées incluent des contrats de parrainage et coordonnées des sponsors, données financières complètes de l'histoire du club, données personnelles et confidentielles des joueurs, stratégies de transfert pour les nouveaux et jeunes joueurs, données confidentielles des fans et des employés, données sur les jeunes sportifs, dossiers médicaux, informations sur les structures et les stades ainsi que les stratégies commerciales et plans d'affaires.

Parmi les documents dérobés, il y a un contrat de travail de Vincenzo Italiano, le manager. Le document contient des informations mentionnant une rémunération annuelle de 4,575 millions d'euros pour cette saison et la saison suivante.

D'autres documents que les auteurs de l'infraction affirment être authentiques incluent le code d'identification fiscale ainsi que le numéro de compte bancaire d'Italiano.

Par ailleurs, un prétendu scan du passeport de l'ancien directeur adjoint Emilio De Leo figure également parmi les échantillons, et la structure des fichiers volés indique que RansomHub pourrait détenir les passeports, les contrats et les informations personnelles des joueurs de l'équipe première du club, remontant au moins à 2017.

En outre, des feuilles de calcul ont été publiées sur le site de fuite de données des cybercriminels (DLS), semblant présenter des détails sur les finances du club, y compris les revenus annuels provenant de divers parrainages ainsi que les sommes attendues et dues à d'autres clubs professionnels de la ligue.

3. Attaques par Social Engineering

3.1. Définition du Social Engineering

Le Social Engineering repose sur le fait de pouvoir exploiter des faiblesses humaines afin de pouvoir contourner des mesures de sécurité. Les attaquants utilisent des mécanismes de manipulation qui ciblent les biais cognitifs tels que la confiance, l'urgence perçue, ou bien l'effet d'autorité. Ce genre de technique permet aux attaquants de pousser les victimes à divulguer des informations ou exécuter des actions compromettantes sans même qu'elles en aient conscience.

L'ingénierie sociale se sert donc de faiblesses comportementales au lieu de vulnérabilités techniques. Par exemple, une personne prétendant être un gestionnaire IT et sollicitant un accès urgent à un système pourrait obtenir des données sensibles si la personne visée ne prend pas le soin de contrôler son identité. Ce phénomène est amplifié par l'excès de charge mentale des salariés et la généralisation des échanges numériques rapides et sans contact physique.

Les cybercriminels améliorent constamment leurs tactiques en s'ajustant aux nouvelles méthodes organisationnelles et aux environnements. Ils mettent en œuvre des méthodes validées tirées de la psychologie sociale, en particulier la théorie de

l'engagement. Cette théorie vise à encourager un individu à réaliser une première action insignifiante avant d'exprimer une demande plus délicate. Ce qui rend ces attaques d'autant plus redoutables est leur aptitude à déjouer les mécanismes de sécurité conventionnels. Un système dûment sécurisé ne sera pas d'une grande valeur si un utilisateur divulgue sciemment ses identifiants à un cybercriminel persuasif. L'ingénierie sociale mets en évidence une vérité : la protection des données s'étend au-delà de la technologie, englobant également le comportement humain. (Wikipédia, 2025)

3.2. Méthodes de manipulation directes

Il y a plusieurs méthodes pour manipuler une personne ou exploiter des failles humaines. Il existe les méthodes directes. Elles reposent sur une interaction entre l'attaquant et la victime, exploitant une approche frontale et souvent opportuniste. Ce genre de méthodes nécessite un canal de communication tels que les appels téléphoniques, les e-mails, les messageries instantanées et parfois, les rencontres en face à face pour établir un contact direct.

Parmi ces méthodes, le phishing est l'une des plus répandues aujourd'hui. Il consiste à inciter une personne à cliquer sur un lien, à télécharger une pièce jointe malveillante ou à divulguer des identifiants sous une fausse page web par exemple. Ce genre d'attaque est souvent une attaque de masse. Les attaquants envoient des millions de mails et attendent que quelqu'un morde à l'hameçon. Parfois, ce genre d'attaque peut aussi être ciblée, c'est « le spear phishing ». Les attaquants ciblent des individus spécifiques avec des messages plus ciblés avec les informations qu'ils ont préalablement collectées.

Une autre méthode est le clone phishing, les attaquants copient des e-mails légitimes déjà reçus par la victime, et remplacent les liens ou les pièces jointes par des éléments malveillants, ce qui augmente la crédibilité de l'attaque.

Une variante élaborée du phishing est le whaling. Cette méthode cible des dirigeants ou des cadres supérieurs en se basant sur des informations de haut niveau et en exploitant la hiérarchie. Contrairement au phishing standard, le whaling repose sur une recherche d'informations précises et une ingénierie sociale approfondie.

Un cyberattaquant peut aussi se faire passer pour un technicien, un prestataire pour essayer de s'infiltrer dans les zones sensibles de l'entreprise telles que des bureaux

avec des ordinateurs déverrouillés, ou des salles serveurs. Une technique courante est le tailgating. L'attaquant profite d'un moment d'inattention pour suivre un employé légitime dans un bâtiment sécurisé sans utiliser de badge en restant proche de la victime.

Vous en êtes sûrement la cible, mais il y a de plus en plus de vishing (hameçonnage vocal) et du smishing (hameçonnage par SMS). Ces nouvelles variantes exploitent la confiance des utilisateurs dans des sources de communication courantes. Les cybercriminels se font passer pour des représentants de la sécurité informatique, des banques ou des administrations afin d'obtenir des informations sensibles en instaurant un climat de légitimité ou bien d'urgence.

Les escroqueries par faux support technique sont aussi courantes. L'intrus se présente comme un professionnel de l'informatique de la société et sollicite des accès ou des renseignements confidentiels sous le prétexte d'entretien ou de mise à niveau. Ces assauts sont fréquemment planifiés avec une minutie remarquable, l'agresseur ayant au préalable rassemblé des renseignements sur la structure et le personnel de l'entité. Il pourrait, par exemple, se présenter avec un faux insigne ou une tenue officielle pour augmenter sa crédibilité. Une version spécifiquement périlleuse consiste à copier le style et les méthodes du véritable service d'assistance interne, rendant la tromperie encore plus complexe à identifier.

Les attaques par récompense ou cadeau exploitent la psychologie humaine en offrant une fausse récompense, comme un bon d'achat, un accès exclusif à un service, un remboursement illusoire ou un prix fictif dans un concours imaginaire. Ces propositions séduisantes sont fréquemment diffusées sous forme de courriels, de publicités numériques ou de publications sur les réseaux sociaux encourageant les individus ciblés à fournir des données personnelles comme des identifiants, des informations bancaires ou des mots de passe.

Parfois, ces attaques se manifestent sous la forme de programmes de fidélité où l'utilisateur est sollicité pour fournir des renseignements confidentiels afin d'accéder à un soi-disant privilège exclusif. Les cyberattaquants peuvent recourir à des fenêtres contextuelles imitant des alertes de système prétendant offrir une récompense en retour de l'installation d'un programme malveillant. Une approche plus raffinée consiste à expédier un colis frauduleux ou à proposer une invitation exclusive pour un événement prestigieux, exploitant la curiosité et le désir de gratification pour tromper la victime.

Le « quizzing » est une tactique discrète où les cybercriminels abusent de la confiance des gens en proposant des faux questionnaires, des concours ou des enquêtes de marché. Les cyberattaquants présente ces sondages comme anonymes ou associés à des entreprises de renom, incitant les victimes à divulguer des renseignements personnels tels que leurs adresses électroniques, numéros de téléphone ou réponses aux interrogations de sécurité. Après leur collecte, ces informations sont exploitées pour mener des attaques spécifiques, comme le phishing. Les cyberattaquants pourraient aussi fusionner ces données avec d'autres informations publiques pour augmenter la crédibilité de leurs manœuvres frauduleuses.

Les faux appels d'urgence sont également une pratique fréquente. Un cyberattaquant contacte un salarié en prétendant être un dirigeant et demandant une action immédiate de la part du salarié, comme l'approbation d'un versement ou l'accès à des données sensibles. Cette méthode est appelée l'arnaque au président. C'est une tromperie qui vise principalement les sociétés. Dans cette situation, le cyberattaquant prétend être un cadre ou un partenaire de haut rang et trompe un employé en évoquant une opération urgente et secrète, généralement assortie d'une interdiction de révéler des informations. L'usage de la position d'autorité et de la contrainte psychologique empêche la victime de vérifier la légitimité de la requête, l'incitant à réagir rapidement, ce qui favorise le détournement de fonds ou l'accès à des données sensibles.

Le shoulder surfing est une autre méthode où un agresseur observe discrètement un utilisateur lors de la saisie de ses identifiants sur un dispositif, fréquemment dans des endroits publics tels qu'une salle de conférence ou un café. (Trevino, 2024)

Les méthodes directes sont vastes. Elles sont très efficaces et très utilisées par les cyberattaquants pour essayer de s'introduire dans le système d'information. Elles exploitent la psychologie humaine, la routine, la pression afin de créer un climat de confiance ou de pression. Il est important de former les utilisateurs et de sensibiliser régulièrement pour atténuer les risques.

3.3. Méthodes de manipulation indirectes

Ils existent aussi les méthodes indirectes. Certaines méthodes visent à exploiter l'environnement numérique et informationnel de la cible pour en extraire des données exploitables ou pour l'influencer à distance. L'une des approches les plus répandues repose sur l'exploitation de l'intelligence en sources ouvertes. C'est l'OSINT (Open

Source Intelligence). Un attaquant peut établir un profil détaillé de sa cible sans avoir besoin d'entrer en contact avec celle-ci en utilisant les informations disponibles publiquement. Une simple analyse des réseaux sociaux professionnels peut permettre de tracer la structure d'une entreprise et de repérer des employés susceptibles d'être ciblés par une tentative de compromission. L'utilisation de forums et de bases de données accessibles au public peut exposer des informations techniques essentielles, rendant ainsi plus facile la préparation d'une attaque spécifique. Cette méthode permet aux attaquants de personnaliser leurs stratégies et d'augmenter leurs chances de réussite.

Après avoir rassemblé ces informations, le cyberattaquant peut utiliser des méthodes de manipulation psychologique plus élaborées, telles que le pretexting. Cette technique s'appuie sur l'élaboration d'un scénario plausible pour encourager la victime à révéler des informations confidentielles. Cette méthode, à l'inverse des attaques traditionnelles qui visent directement les accès secrets, fait appel à la confiance et à l'autorité. En se faisant passer pour un spécialiste en informatique ou un expert en sécurité des systèmes d'information, un cyberattaquant peut facilement persuader un salarié de lui remettre ses identifiants en faisant passer cela sous la maintenance ordinateur ou mise à jour d'un logiciel. Cette technique fonctionne en tirant parti du sentiment d'urgence et de l'effet d'autorité, rendant fréquemment la cible incapable de prendre du recul pour remettre en question la requête. De plus, le pretexting peut être modulé en fonction de différents contextes, notamment en recourant à des situations plausibles comme un incident technique inattendu, une mise à jour essentielle de sécurité ou une requête de vérification administrative.

Certaines attaques indirectes n'exigent même pas une sollicitation directe de la victime. Ce sont les attaques par watering hole, qui visent à infiltrer un site web souvent fréquenté par les employés d'une société pour y insérer un code malintentionné. En guidant les utilisateurs vers une ressource compromise, les malfaiteurs peuvent obtenir un accès sans avoir à déjouer les systèmes de protection internes. Ces attaques ciblent spécifiquement les portails internes des sociétés, les plateformes SaaS employées en milieu professionnel, ainsi que les sites web de fournisseurs externes dont la compromission est souvent difficile à détecter.

Il y a aussi une technique très comparable que j'ai d'ailleurs pu observer en pratique lors de mon contrat d'apprentissage. Le « typosquatting » ou « attaque par domaine lookalike », qui est une technique d'intrusion indirecte, vise à adopter un nom

de DNS proche de celui de l'entreprise. L'objectif est qu'un employé potentiel de l'entreprise ciblée se connecte spontanément et saisisse ses propres informations d'identification. Il est aussi possible d'essayer d'usurper les sites web d'une entreprise en utilisant un nom de domaine proche. (Proofpoint, s.d.)

Pour finir, une approche délicate et encore peu explorée touche à l'empoisonnement des données. Les agresseurs insèrent des données incorrectes dans les bases de données ou les systèmes d'analyse pour perturber les décisions stratégiques. Cette méthode s'adapte parfaitement aux contextes où l'intelligence artificielle et le machine learning sont utilisés, car l'insertion de données biaisées peut déformer les modèles prévisionnels et provoquer des dysfonctionnements systématiques. Ces interventions peuvent se manifester sous diverses formes, depuis la manipulation de paramètres financiers jusqu'à la modification d'indicateurs de performance, influençant par conséquent les directions stratégiques des entités touchées.

3.4. Exemples de campagnes de phishing réussies

En 2020, lors des Jeux Olympiques de Tokyo, une campagne d'hameçonnage a permis aux cybercriminels d'accéder à des systèmes d'informations contenant les informations médicales sensibles des athlètes. L'attaque a débuté avec des e-mails malveillants qui ressemblaient à des messages officiels provenant d'organismes sportifs et médicaux. Les destinataires étaient invités à contrôler ou actualiser leurs dossiers médicaux électroniques en s'authentifiant sur une plateforme malveillante.

Lorsque les victimes cliquaient sur les liens de ces emails, elles étaient dirigées vers des pages d'authentification trompeuses qui enregistraient leurs identifiants. Cela a permis aux attaquants d'accéder aux bases de données médicaux des athlètes de différents sports. Ces données étaient composées de secrets médicaux, de tests de dopage, d'informations personnelles. Certaines des informations exfiltrées ont notamment été publiées sur le darkweb, des forums publics. Cela a créé une mauvaise réputation, ainsi que des spéculations de la part des fans. Ces divulgations ont terni la réputation de plusieurs athlètes, certains étant injustement soupçonnés de dopage suite à l'exposition de traitements médicaux secrets.

Lors de la Coupe du Monde de football 2022 au Qatar, les équipes de cybersécurité ont observé de nombreuses campagnes d'hameçonnage. Ces campagnes avaient pour cibles les joueurs, les entités sportives, les prestataires, ainsi que les fans.

Une des campagnes les plus efficaces a été d'envoyer des e-mails malveillants en encourageant les destinataires à installer une application mobile. Ils ont fait croire dans les mails que cette application allait leur permettre de suivre les matchs gratuitement et de bénéficier d'offres promotionnelles. Cependant, l'application renfermait un logiciel malveillant qui permettait aux attaquants de récupérer les identifiants, les mots de passe utilisateurs. Cela leur a permis de prendre la main sur des comptes de réseaux sociaux, des comptes de mails, des comptes bancaires.

Une autre campagne d'hameçonnage avait pour but de prétendre de faire partie des services de billetterie officiels de la Coupe du Monde. Des milliers de fans ont reçu des courriels comportant de faux liens de paiement pour récupérer ou valider leurs tickets électroniques. Les victimes étaient dirigées vers des sites trompeurs où elles étaient invitées à saisir leurs informations financières.

Selon un autre incident rapporté par le National Cyber Security Centre (NCSC), des cybercriminels ont profité de comptes de messagerie compromis détenus par des employés techniques de clubs de football pour transmettre des e-mails aux joueurs. Les e-mails avaient pour but de demander aux joueurs à se connecter à une fausse plateforme de gestion des contrats et des salaires. Après avoir dérobé les identifiants, les cybercriminels ont réussi à altérer les informations bancaires des joueurs et à se procurer leurs salaires en détournant et changeant les informations bancaires.

4. Attaques sur les objets connectés (IoT)

4.1. Vulnérabilités des wearables et dispositifs IoT

Les objets connectés couvrent aujourd'hui des matériels très divers. Cela peut aller du pacemaker à la montre connectée, en passant par les caméras, les systèmes industriels, les équipements de domotique grand public et bien d'autres. De tels dispositifs présentent des risques qui peuvent être perçus comme nouveaux du fait de leur capacité à produire des effets physiques en dehors des systèmes d'information. Ces appareils physiques reçoivent et transfèrent des données sur des réseaux sans fil, avec une intervention humaine limitée. Selon une étude récente de SonicWall, un expert en solutions de cybersécurité, une augmentation de 30 % du nombre d'attaques par malware visant l'IoT a été constatée en 2020 pendant la crise sanitaire du COVID-19. Les IoT sont souvent la cible d'attaques de type Déni de Service Distribué afin de rendre impossible l'exploitation de l'objet connecté.

En 2016, le botnet Mirai a été utilisé pour réaliser une des attaques DDoS les plus violentes jamais enregistrée. Les victimes sont l'hébergeur français de sites web OVH et la société Dyn. Cette attaque a paralysé pendant plusieurs jours de nombreux sites et services tel que Twitter, PayPal, Airbnb. Le fonctionnement de Mirai se fondait sur la recherche permanente d'adresses IP correspondant à des objets connectés et vulnérables.

4.2. Piratage de l'application Strava

L'application Strava est une application utilisée pour suivre les sorties avec une trace GPS. Les sorties peuvent être de la course, de la natation, du vélo et d'autres. Il est possible ensuite d'analyser les sorties en retrouvant le nombre de kilomètres, le dénivelé, le rythme cardiaque. La trace GPS est ensuite mise sur votre profil. Si votre profil est public, tous les utilisateurs peuvent accéder à votre parcours, le départ et l'arrivée. Le cas de Strava est un cas particulier. Les problèmes qu'il y a eu ne sont pas liés à une vulnérabilité technique, logicielle, une faille, une zero-day. C'était une vulnérabilité humaine. En effet, je vais vous présenter deux vulnérabilités que des cyberattaquants ont pu exploiter librement via l'application Strava.

Dans une enquête nommée « StravaLeaks », des internautes ont réussi à remonter la trace d'une dizaine de gardes du corps des présidents Emmanuel Macron, Vladimir Poutine et Joe Biden. Les membres du Secret Service sont des sportifs, et certains d'entre eux utilisent l'application Strava. Les gardes du corps et les membres du Secret Service se rendent aux emplacements de réunions, de vacances, de déplacements avant l'arrivée des présidents. Il est donc possible d'identifier à l'avance les lieux où s'apprêtent à séjourner Joe Biden ou Emmanuel Macron par exemple. Ce genre d'informations pourrait être utilisé pour faire pression sur ces agents et mettre en péril la sécurité du président par un individu mal intentionné.

En novembre 2017, l'application Strava a créé une carte thermique de l'ensemble du globe sur la base des données GPS de ses utilisateurs. Cette publication, fondée sur plus de trois mille milliards de points de localisation, a entraîné la révélation involontaire d'informations sensibles concernant plusieurs bases militaires américaines et sites de renseignement. L'analyse des activités générées par cette carte a montré que des bases militaires en Syrie, en Irak et en Afghanistan pouvaient facilement être identifiées grâce aux exercices sportifs des militaires sur site. La figure 9 est une carte qui représente le parcours de plusieurs militaires qui font des courses matinales.

Figure 9, Base militaire, en Afghanistan, cartographié grâce à Strava

Cette erreur humaine a permis de révéler et de cartographier des installations secrètes. Par la suite, Strava a recommandé à tous les utilisateurs militaires de désactiver les paramètres de partage de données.

5. Vol et divulgation de données sensibles

5.1. Piratage de base de données des athlètes

Une base de données est un ensemble d'informations qui est organisé de manière à être facilement accessible, géré et mis à jour. Elle est utilisée par les organisations comme méthode de stockage, de gestion et de récupération de l'information. Les bases de données des infrastructures sportives contiennent des informations sensibles telles que les programmes d'entraînement, les données de santé, et les renseignements personnels. Une fois compromises, ces informations peuvent être utilisées pour manipuler des compétitions, extorquer de l'argent à des athlètes ou diffuser ces informations publiquement afin de nuire à la réputation des sportifs et des institutions.

Les attaques sur les bases de données suivent le même fonctionnement d'attaque que les rançongiciels vus précédemment. Les attaquants essaient de s'infiltrer par une faille de sécurité technique ou humaine. Ils essaient d'obtenir des accès administrateurs

puis d'accéder aux bases de données pour exfiltrer les données. Les attaquants peuvent divulguer les données, les tests médicaux ou des traitements spécifiques. Cela peut entraîner des accusations infondées ou des scandales liés à des soupçons de dopage. De plus, l'exposition de données personnelles, comme les adresses ou les informations familiales, augmente le risque de harcèlement ou d'extorsion. Pour les organisations sportives, ces incidents érodent la confiance des athlètes, des sponsors et du grand public, tout en les exposant à des sanctions juridiques pour manquement à la protection des données.

5.2. Fuites de données sur la santé ou la stratégie d'entrainement

En 2016, dans le cadre des Jeux Olympiques de Rio, une fuite d'information a eu lieu sur les données de 26 sportifs. L'agence mondiale antidopage (AMA) a confirmé que le groupe de cyberespions, « Fancy Bear », a publié un bloc de données confidentielles sur certains sportifs. Les cyberespions ont pu accéder à un compte utilisateur grâce à l'hameçonnage. Ils ont pu obtenir des informations concernant 41 sportifs provenant de 10 pays. Selon l'AMA, cette attaque aurait été conduite par des attaquants réputés russes en réponse aux publications de l'agence révélant un système de dopage institutionnalisé dans le monde du sport russe. Ces révélations ont conduit à l'exclusion d'athlètes russes des compétitions sportives internationales. Le but était de discréditer les efforts antidopage internationaux et de semer le doute sur l'intégrité des compétitions sportives. (Finkle, 2016)

En 2005, un scandale d'espionnage a éclaté en Grèce lors des Jeux Olympiques d'Athènes. Le scandale est nommé « The Athens Shadow Games ». La NSA a aidé la Grèce à mettre en place un système de surveillance pour les Jeux Olympiques d'Athènes 2004, mais au lieu d'être désactivé après l'événement, il aurait été utilisé pour espionner le gouvernement grec. L'enquête a commencé lorsque Vodafone a découvert qu'un logiciel malveillant a infiltré les systèmes télécom. Ce programme permettait d'intercepter secrètement 106 numéros sensibles. L'enquête révèle que les écoutes auraient opérées depuis l'ambassade américaine à Athènes et qu'un agent présumé de la CIA, William Basil, aurait organisé l'opération. Un mandat d'arrêt international a été émis contre cet agent en 2014, mais il a disparu avant d'être arrêté. Par la suite, Vodafone a été condamnée à plus de 100 millions d'euros d'amende pour manquement à la sécurité. (Diaries, EP 64 : The Athens Shadow Games, 2020)

En décembre 2016 et novembre 2018, plus de 18,6 millions de documents relatifs au fonctionnement des instances internationales de football ont fait l'objet de divulgations, communément appelées « Football Leaks ». Les données ont été obtenues au moyen de compromissions de systèmes d'information, mais les détails de ces accès malveillants ne sont pas connus dans les sources ouvertes. Ces révélations ont dévoilé des mécanismes d'évasion fiscale, des soupçons de fraude, de corruption et de dopage. Elles ont ainsi nui à l'image des entités et des individus impliqués. (AFP, s.d.)

6. Attaques d'applications web

Les applications et technologies web sont devenues un élément central des infrastructures sportives. Les sites vitrines, les billetteries, les réseaux sociaux, les forums sont des ressources intégrées aux infrastructures sportives. L'augmentation de la complexité des applications web et la généralisation de leurs services créent des difficultés pour les protéger contre des menaces aux motivations diverses, allant du dommage financier à la dégradation de la réputation, sans oublier le vol d'informations essentielles ou privées et les visées politiques comme le cas russe ci-dessus.

Les applications et services en ligne reposent principalement sur des bases de données pour conserver ou fournir les renseignements nécessaires. Sur la figure 10, il est présenté les vecteurs d'attaque d'application web les plus courants.

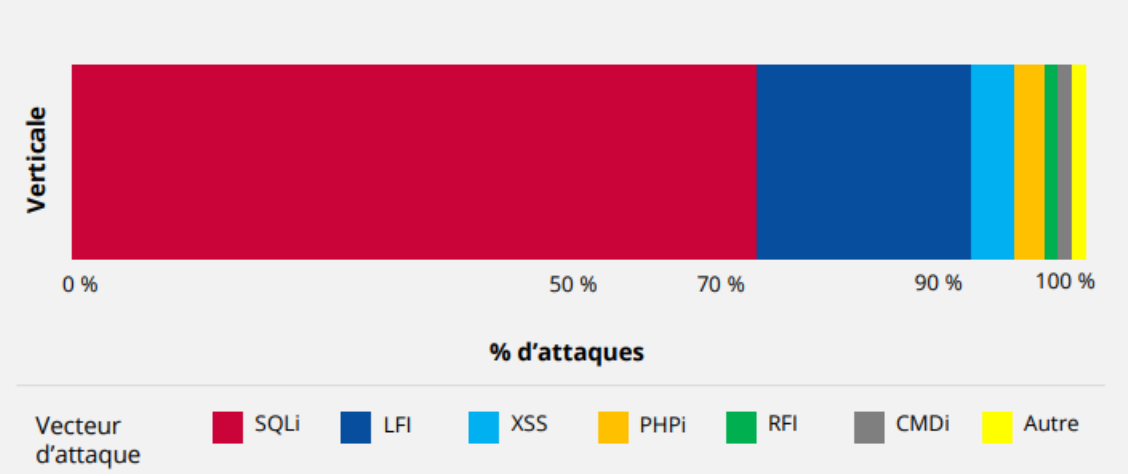

Figure 10, Pourcentage d'attaques d'applications web

(Akamai, 2024)

Les attaques SQLi consistent à insérer des requêtes SQL malveillantes dans un champ de saisie ou une URL afin d'exploiter des failles de sécurité dans une base de données. Un attaquant peut ainsi manipuler les requêtes exécutées par l'application, récupérer des informations sensibles (identifiants, mots de passe), modifier des données ou même supprimer des tables entières. L'attaque repose sur un mauvais filtrage des entrées utilisateur.

Les attaques par Local File Inclusion permettent à un attaquant d'accéder à des fichiers présents sur le serveur en exploitant une faille dans l'application web. En manipulant un paramètre d'URL qui inclut un fichier sans vérification adéquate, il peut lire des fichiers sensibles (comme passwd sous Linux), exécuter du code malveillant ou même obtenir un accès au serveur.

Les attaques par Cross-Site Scripting consistent à injecter du code JavaScript malveillant dans une page web, qui sera ensuite exécuté par les navigateurs des visiteurs. Cette attaque peut servir à voler des cookies de session, rediriger l'utilisateur vers un site malveillant ou afficher des contenus frauduleux. Il y a le XSS stocké (le script est sauvegardé sur le serveur), le XSS réfléchi (le script est exécuté immédiatement via une URL piégée) et le XSS DOM (modification dynamique du DOM via JavaScript).

Les attaques PHP Injection permettent à un attaquant d'exécuter du code PHP arbitraire sur un serveur vulnérable. Cela peut être fait via une entrée utilisateur mal sécurisée qui est directement interprétée par PHP, permettant ainsi d'exécuter des commandes système, de modifier des fichiers ou d'obtenir un contrôle total du serveur.

Alors que les organisations deviennent de plus en plus compétentes dans le développement d'une automatisation plus cohérente du cycle de vie de leurs applications web, elles exigent désormais que la sécurité soit l'élément primordial de leur offre et au centre de leurs priorités. Cette introduction d'environnements complexes favorise l'adoption de nouveaux services, comme les interfaces de programmation d'applications (API - Application Programming Interfaces). Les API, qui créent de nouvelles problématiques pour la sécurité des applications web, peuvent nécessiter d'autres mesures de prévention et de détection. Ainsi, environ 80 % des organisations utilisant des API ont déployé des contrôles sur leur trafic entrant. (Radware, 2024)

III. Les protections associées

1. Mesures organisationnelles

1.1. Mise en place d'un cadre de gouvernance en cybersécurité

La mise en place d'un cadre de gouvernance en cybersécurité au sein des infrastructures sportives est essentielle pour garantir une protection efficace contre les menaces numériques. Il est important de définir les rôles et les responsabilités des responsables IT, des dirigeants, du personnel administratif ainsi que des partenaires. Une gouvernance repose sur une bonne collaboration entre les différentes parties prenantes. Le but est de pouvoir garantir une protection cohérente et adaptée aux risques du secteur sportif.

L'approche EBIOS Risk Manager peut être utilisée pour identifier et hiérarchiser les risques en fonction de leur impact potentiel sur l'organisation. Cette méthode permet d'évaluer les menaces et de définir des mesures en fonction de chaque risque. Elle permet de renforcer la résilience des infrastructures sportives en simulant des scénarios d'attaques et de crises. Cela permet d'établir différents plans et procédures à adopter en fonction de la crise.

En parallèle, l'application des normes et standards de cybersécurité, tels que l'ISO/IEC 27001, le RGPD ou encore le NIST Cybersecurity Framework, permet de mettre en place un cadre de cybersécurité. Lors de la mise en place de ces normes, il est obligatoire d'effectuer des audits réguliers du système. Cela permet de détecter les vulnérabilités et d'assurer une amélioration continue des équipements mis en place.

Enfin, l'intégration de la cybersécurité dans la gouvernance des événements sportifs d'envergure tels que les Jeux olympiques et des championnats du monde se fait grâce à une collaboration étroite entre les agences gouvernementales, les prestataires de service et les acteurs privés.

1.2. Sensibilisation et formation de la trésorière et du président du club de Badminton Castelpontin

Comme je vous l'ai montré lors du chapitre précédent sur les attaques fréquentes dans le monde du sport, le principal point d'entrée est l'erreur humaine. Il est important de former les utilisateurs, le personnel, les sportifs sur les risques liés à l'informatique. J'ai notamment eu l'opportunité de réaliser une session de sensibilisation auprès du

trésorier et le président du Club de Badminton Castelpontin à Pont du château. Lors de cette session, j'ai pu les sensibiliser sur les points que je vais aborder ci-dessous.

Dans un premier temps, je leur ai présenté les différents types d'attaques possibles. J'ai pu leur expliquer le phishing, les rançongiciels, les attaques par déni de service distribué, l'ingénierie sociale, les malwares sur mobiles, le cryptojacking. Je les ai sensibilisés sur les types d'attaques du moment tels que les faux ordres de virement, le smishing, les QR Code, l'arnaque au président, l'escroquerie au test informatique, l'arnaque au « faux le Drian », l'escroquerie aux coordonnées fournisseurs. Les signes d'une attaque sont les suivants, un virement non planifié et inhabituel, un changement de RIB intempestif d'un fournisseur, un prétexte urgent souvent accompagné de nombreux détails et d'un style inhabituel (flatterie ou menace), et l'usurpation d'identité d'une personne de confiance.

Dans un second temps, je les ai sensibilisés sur les mots de passe. Il est important de créer un mot de passe robuste pour éviter les attaques. L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe. Il s'agit de tester, une à une, toutes les combinaisons possibles. Les attaques par dictionnaire sont utilisées en cryptanalyse pour trouver un mot de passe ou une clé. Elles consistent à tester une série de mots de passe potentiels, les uns à la suite des autres, en espérant que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Enfin, les fuites de données lorsque des hackers obtiennent une base de données de comptes volés. Les logins, mots de passe, informations personnelles peuvent être piratés et exposés sur internet. Il est notamment possible de vérifier cela sur les sites comme haveibeenpwned ou leaklookup. Sur la figure 11, il y a 2 tableaux de Hive Systems qui présentent le temps qu'il faut à un attaquant pour trouver votre mot de passe avec IA et sans IA.

SANS IA

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

HIVE SYSTEMS › Learn how we made this table at hivesystems.com/password

AVEC IA

USING CHATGPT HARDWARE TO BRUTE FORCE YOUR PASSWORD IN 2023

Hardware: 10,000 x A100's | Password hash: MD5

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 sec
9	Instantly	Instantly	4 secs	21 secs	1 min
10	Instantly	Instantly	4 mins	22 mins	1 hour
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hour	12 months	10 years	47 years
14	Instantly	1 day	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

HIVE SYSTEMS › Learn more about this at hivesystems.com/password

Figure 11, Temps pour trouver un mot de passe avec IA et sans IA

(Neskey, s.d.)

J'ai vu avec eux afin qu'ils puissent installer un coffre-fort de mot de passe à la fois sur les ordinateurs mais aussi sur les téléphones. J'ai fait le choix de prendre BitWarden qui est compatible MAC, Windows, Linux, Android et iPhone. J'ai installé avec eux le logiciel sur ordinateur, téléphone, ainsi que l'extension pour le navigateur. Ensuite, je leur ai appris à générer des mots de passe robustes pour les comptes Microsoft, les comptes de fédération de badminton, les comptes de réseaux sociaux. Je leur ai appris à créer un mot de passe robuste pour le déverrouillage du PC et le mot de passe maitre du coffre-fort. J'ai repris les recommandations de l'ANSSI. Les mots de passe contiennent 12 caractères de type différent (majuscules, minuscules chiffres, caractères spéciaux) n'ayant aucun lien avec la personne (nom, date de naissance). Je leur ai appris deux méthodes. La première est la méthode phonétique. Si je prends la phrase « J'ai acheté 5 CDs pour cent euros cet après-midi ». Le mot de passe sera « ght5CDs%€7am ». La deuxième méthode est celle des premières lettres. Si je prends la phrase « Allons enfant de la patrie, le jour de gloire est arrivé ». Le mot de passe sera « aE2lP,lJ2Géa ! ».

Et enfin, j'ai terminé cet atelier de sensibilisation sur les aspects « publics ». En effet, ils n'ont pas de réseau interne, de pare-feu, de serveurs. Les locaux sont souvent publics, il y a beaucoup de personnes qui viennent et qui partent. Il est donc important

de verrouiller son ordinateur et de ne pas se connecter au Wi-Fi publics. Il existe quelques gros problèmes avec l'utilisation des réseaux Wi-Fi publics. Le réseau, ouvert par défaut, est vulnérable aux tentatives d'espionnage, le réseau pourrait être rempli de machines infectées. Si vous êtes connecté à un site en HTTPS, les communications sont chiffrées et vos informations personnelles sont illisibles sur le réseau local. Malheureusement il reste possible pour un intrus de savoir sur quel site vous êtes. Les attaquants peuvent créer un Wi-Fi public qui reste ouvert et donc accessible sans mot de passe. Il est là pour vous attirer. Le danger est que ce réseau est totalement sous le contrôle du pirate informatique : il peut alors voir tout ce que vous y faites et voler vos informations. Il est aussi possible de partager un fichier avec des virus sur les smartphones ou sur les ordinateurs. Avec un iPhone ou un Mac, vous pouvez recevoir un fichier d'un inconnu via AirDrop. Il est fortement recommandé de ne jamais accepter ces partages car ces fichiers sont très souvent infestés de virus. L'attaquant est capable de créer une fausse notification de mise à jour qui est envoyée sur votre appareil via un Wi-Fi public. Ces notifications concernent souvent un outil à mettre à jour sur votre téléphone en cliquant sur un lien ou un bouton. Si vous le faites, vous vous exposez à une infection avec des virus qui pourraient compromettre votre navigation, vos données et vos informations personnelles.

1.3. Développement de politiques internes de sécurité

Les politiques internes de sécurité définissent les règles et procédures à suivre pour protéger les actifs, données et systèmes de l'entreprise contre les menaces et les risques. Au sein du Groupe Titel, j'ai pu mettre en place différentes politiques internes de sécurité.

J'ai pu mettre en place une politique de mot de passe robustes de 12 caractères de type différent (majuscules, minuscules chiffres, caractères spéciaux) sans lien direct avec l'utilisateur (nom, date de naissance). Les mots de passe doivent être renouvelés tous les 3 mois. Cette politique est à la fois écrite dans la documentation, mais elle est mise en place via des stratégies de groupes sur l'Active Directory. J'ai rendu obligatoire la mise en place de la double authentification sur les comptes privilèges Microsoft 365. Il existe aussi des politiques de gestion des comptes et privilèges, de politique de gestion des accès physiques.

J'ai installé un plan de sauvegarde et de restauration. Ce plan recense les sauvegardes effectuées de notre logiciel VEEAM, avec les dates, le type de sauvegarde, le

stockage. Cela permet de savoir précisément où sont stockés les sauvegardes, la durée de rétention, ainsi que les différents supports de stockage. Il est aussi possible de mettre en place des politiques de chiffrement des données qui imposent l'usage du chiffrement pour protéger les données en transit et au repos.

Il est important d'établir des politiques BYOD (Bring Your Own Device) qui permettent d'encadrer l'utilisation des appareils personnels sur le réseau de l'entreprise, notamment les smartphones, les tablettes, les ordinateurs portables. Elles définissent les règles d'accès aux ressources de l'entreprise via ces dispositifs, notamment en termes de sécurité, d'accès aux données sensibles. Les politiques de mise à jour et de correction des vulnérabilités définissent la fréquence des mises à jour. L'objectif est de corriger les vulnérabilités de sécurité dès qu'elles sont découvertes par les éditeurs de logiciels. Elles s'appliquent à l'ensemble des équipements et des dispositifs connectés à l'infrastructure. Je n'ai malheureusement pas encore eu le temps d'approfondir ce sujet et de déployer des règles sur le BYOD.

Les politiques de segmentation des réseaux visent à limiter l'exposition aux cyberattaques en séparant les différents réseaux internes de l'entreprise. J'ai mis en place différents réseaux séparés par des réseaux virtuels appelés VLAN. Cela m'a permis de scinder la partie bureautique, serveur, production, Wi-Fi public, Wi-Fi privé, téléphonie, imprimante. Cette segmentation permet de réduire l'impact d'une éventuelle compromission d'une partie du réseau. (IBM, 2024)

Et enfin, les politiques de réponse aux incidents et de continuité définissent les procédures et actions à suivre lorsque survient un incident de sécurité (comme une cyberattaque, une fuite de données, une panne système). Leur but est de minimiser l'impact de l'incident sur l'entreprise, de contenir l'incident rapidement, et de remettre en place les services essentiels. J'ai notamment pu commencer à rédiger et établir un Plan de Reprise d'Activité (PRA). Ce plan établit les actions pour restaurer les services informatiques après un incident majeur. Ainsi qu'un Plan de Continuité d'Activité (PCA), qui assure le maintien des opérations essentielles en cas de crise.

2. Mesures techniques

2.1. Gestion des accès et des identités numériques

2.1.1. Multi-Factor Authentification (MFA)

L'authentification simple repose sur un seul facteur. Par conséquent, si cet unique facteur d'authentification est compromis, un pirate pourra accéder librement à votre compte en ligne et aux données qu'il contient. Cela explique que les premières cibles d'attaque des pirates informatiques soient les identifiants de connexion (identifiant de compte, le plus souvent une adresse mail et le mot de passe). Le fait de disposer de ces informations augmente leurs chances d'accéder à vos autres comptes, de voler vos données personnelles, notamment bancaires ou sensibles et d'usurper votre identité. Cela conduit à des vols fréquents de bases de données comportant des identifiants et des mots de passe. C'est également un des objectifs des attaques par hameçonnage.

L'authentification multifacteur permet de renforcer la sécurité de l'accès à vos comptes grâce à l'ajout d'un ou de plusieurs facteurs d'authentification. L'utilisation de l'authentification multifacteur rend plus difficile le piratage d'un compte. En effet, même si un pirate informatique parvient à se procurer votre identifiant et votre mot de passe, il ne pourra pas accéder à votre compte, faute de disposer du second facteur d'authentification. L'authentification multifacteur met en œuvre un facteur d'authentification supplémentaire associé à votre compte « à ce que vous savez » (un mot de passe, par exemple) peut se combiner « à ce que vous possédez ». Par exemple, un code reçu par mail, un code reçu par SMS, un jeton USB, une carte à puce, une empreinte biométrique, la reconnaissance faciale.

Cette méthode de sécurisation se met en place en créant un lien entre l'appareil ou l'application à laquelle l'utilisateur souhaite se connecter, et le support servant de vérificateur de son identité. J'ai pu mettre en place cette technologie sur les comptes Microsoft d'administrateur de mon entreprise. La figure 12 présente la mise en place de l'authentification multifacteur par utilisateur sur le domaine du Groupe TITEL.

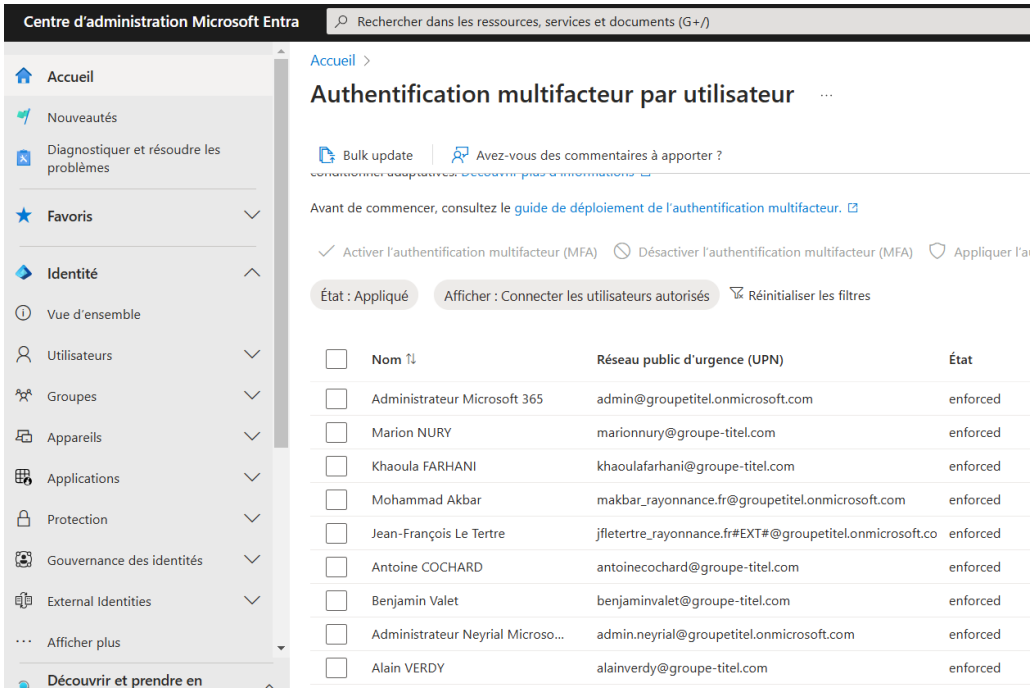

Figure 12, Authentification multifacteur par utilisateur du Groupe TITEL

J'ai fait le choix de mettre en place cette configuration pour les administrateurs du tenant Microsoft 365. Mais j'ai aussi poussé cette configuration à nos prestataires (Neyrial et Rayonnance). Cela a permis d'augmenter la sécurité sur les comptes d'administrations. Cependant, il n'est pas encore possible de l'activer pour tous les utilisateurs. C'est un projet que j'ai en cours. Il n'est pas possible de le mettre en place via leurs téléphones portables personnels. Je vais devoir trouver un moyen avec des clés USB, des Yubikey ou autre.

2.1.2. Gestion des privilèges d'accès

La gestion des privilèges d'accès est un élément important dans la sécurité des systèmes d'information d'infrastructure sportive ou d'entreprise. Cette sécurité repose sur le principe de moindre privilège. Chaque utilisateur ne doit disposer que des droits strictement nécessaires à l'exécution de ses tâches. Les droits d'accès sont attribués en fonction des rôles et des responsabilités des utilisateurs. Le personnel du service informatique nécessite un accès aux infrastructures critiques, les entraîneurs et analystes doivent accéder aux données de performance des athlètes, tandis que les athlètes disposent d'un accès limité à leurs propres informations.

La méthode principale utilisée dans les systèmes d'information est la gestion des droits, des groupes et des dossiers partagés par l'Active Directory. Depuis l'Active

Directory, il est possible de créer des utilisateurs, des groupes d'utilisateurs, des groupes spécifiques. Des droits en lecture, écriture et/ou exécution sont créés. Puis un ou plusieurs groupes sont attribués à un utilisateur. Cela permet de gérer les droits sur les dossiers partagés facilement. (CyberArk, 2023) Sur la figure 13, j'ai inséré une courte liste d'utilisateur de l'Active Directory du Groupe TITEL, ainsi que des groupes de sécurité, et enfin les propriétés du compte d'Antoine Cochard.

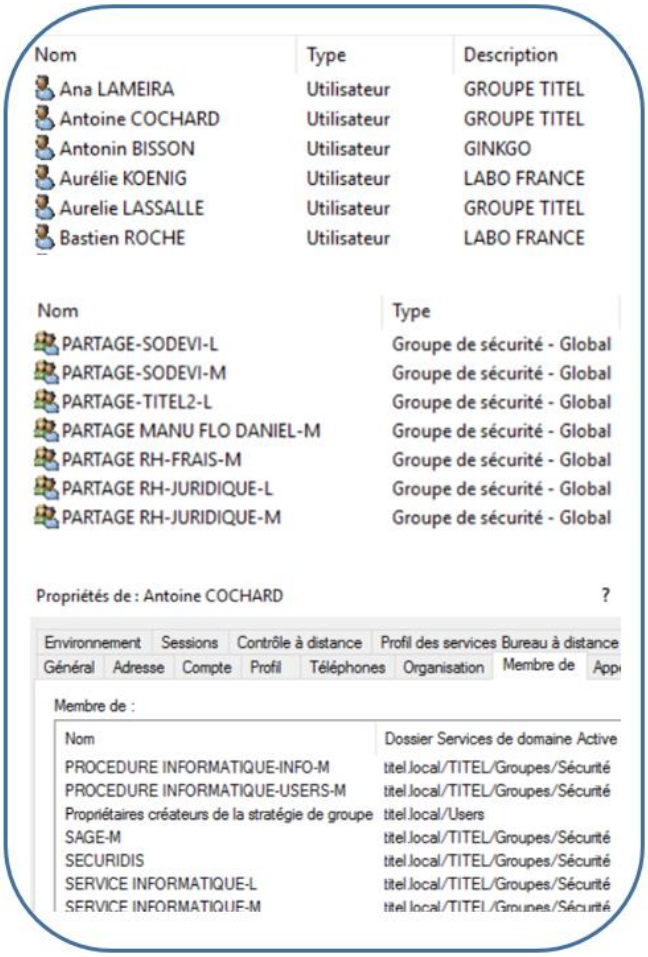

Figure 13, Utilisateurs, groupes et propriétés de l'utilisateur Antoine Cochard

Cela permet d'ajouter au compte Antoine Cochard différents groupes. Ces groupes sont ensuite ajoutés dans les propriétés des dossiers partagées. La figure 14 présente les propriétés des dossiers partagés et notamment celui du service informatique. Comme je vous l'ai expliqué précédemment, ce dossier comporte des propriétés de modification, lecture et exécution, d'affichage et de contrôle total. Il est donc possible de créer différents groupes pour restreindre et adapter au mieux les accès des utilisateurs.

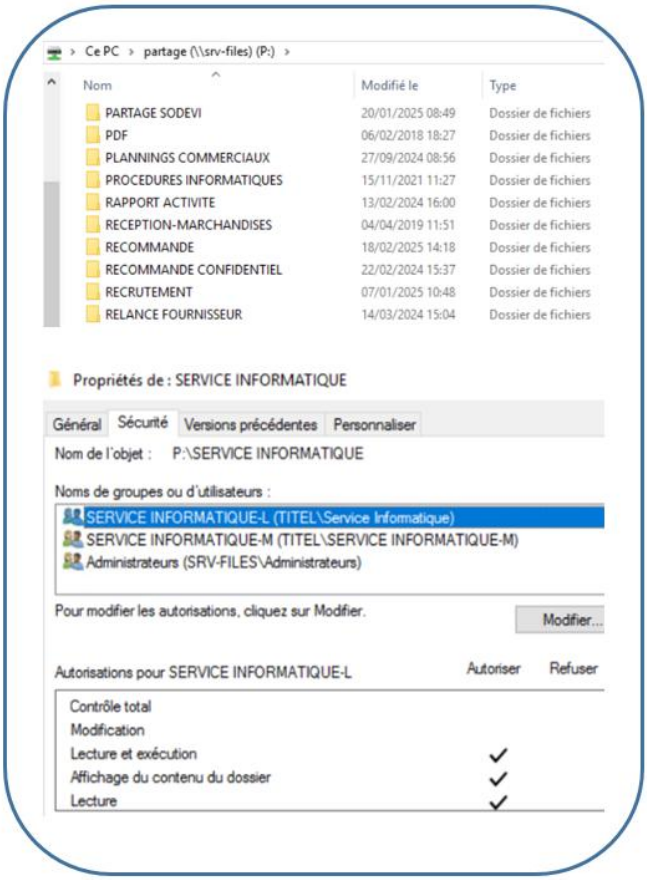

Figure 14, Propriétés des dossiers partagés

L'avantage des dossiers partagés est la possibilité de personnaliser les accès et les restrictions selon le besoin. L'inconvénient est que cette gestion est souvent faite de manière manuelle et donc elle oblige à modifier régulièrement les membres des différents groupes selon les arrivées, les départs, les changements de postes dans l'organisation.

2.2. Segmentation des réseaux sportifs

2.2.1. Architecture Zero-Trust

Le modèle Zero Trust est une approche architecturale visant à renforcer la sécurité d'accès aux services, aux serveurs et ressources d'un système d'information. Les modèles traditionnels accordent une confiance aux utilisateurs situés à l'intérieur du réseau. Tandis que le modèle Zero Trust remet en question cette confiance en considérant que chaque tentative interne ou externe d'accès doit être vérifiée.

Cette approche est souvent utilisée dans les infrastructures sportives étant donné que ces architectures utilisent énormément le cloud, le télétravail, les outils personnels

(BYOD). Le Zero Trust permet de mettre l'accent sur la vérification continue des accès aux ressources. L'accès aux ressources doit être contrôlé en fonction des besoins de chaque utilisateur en appliquant le principe du moindre privilège. Ensuite, chaque demande d'accès doit être évaluée indépendamment de l'origine, qu'elle provienne de l'intérieur ou de l'extérieur. Les politiques d'accès doivent être dynamiques afin de prendre en compte l'identité de l'utilisateur, la sensibilité de la ressource demandée, l'analyse comportementale ou enfin l'heure et la localisation de la demande. Enfin, les processus d'authentification et d'autorisation doivent être mis à jour afin d'être confiants sur leur pertinence et leur efficacité.

La barrière entre les appareils professionnels et personnels est parfois très faible, surtout dans le milieu sportif ou associatif. Le modèle Zero Trust permet de rester vigilant face à ces risques. Ce modèle empêche la propagation des cyberattaques, réduit les coûts de remédiation et facilite la conformité aux réglementations. En améliorant la visibilité et la gestion des accès, il protège les athlètes, les équipements connectés et les systèmes critiques tout en garantissant la continuité des événements sportifs.

2.2.2. Ségrégation des réseaux

Les infrastructures sportives modernes possèdent plusieurs réseaux différents. Je vous ai précédemment présenté l'architecture interne du réseau du Clermont-Foot. Il y avait un réseau dédié à la partie administrative, à la partie IoT, aux caméras, aux flux vidéos et enfin au Wi-Fi. La segmentation permet d'isoler les différentes zones et de limiter la propagation d'attaques en cas de compromission. Il est aussi possible de pouvoir allouer une ou plusieurs arrivées internet pour un réseau en particulier (flux vidéos par exemple). Il sera donc possible d'attribuer plus de débit aux flux vidéos et aux caméras lors des événements sportifs et moins à la partie administrative.

La segmentation physique des réseaux est réalisable en utilisant différentes arrivées internet, différents câbles. Mais il est aussi possible de segmenter virtuellement les réseaux en utilisant les VLANs. Les VLANs (ou Virtual Local Area Network) sont un outil en réseau qui permet de segmenter un réseau en plusieurs sous-réseaux virtuels afin de s'adapter aux besoins de l'entreprise. Cette segmentation permet d'isoler les différents sous-réseaux, mais aussi de renforcer la sécurité, gérer le trafic et de structurer le réseau de manière plus efficace.

Le fonctionnement des VLANs consiste à ajouter une étiquette aux paquets réseau contenant les données afin d'associer ces paquets à un VLAN spécifique au sein d'une trame réseau. Ceci s'appelle l'encapsulation. Les VLANs sont gérés par les switchs, routeurs et pare-feux qui vont guider les trames réseau selon leurs étiquettes, ce qui permet donc d'organiser et de segmenter le réseau et le trafic. De cette manière, seules les machines présentes dans un VLAN précis sont concernées par les trames et les règles qui s'en rapportent. Pour que les appareils souhaités soient associés à un VLAN particulier, les ports qui les lient au switch doivent être configurés d'une certaine manière. Il est possible ensuite de pouvoir faire communiquer les VLANs entre eux. C'est le routage Inter-VLAN. Les VLANs peuvent être créés et gérés par le pare-feu ou bien par le routeur. Ils sont ensuite mis en place sur des switchs. J'ai notamment pu mettre en place des VLANs pour scinder les réseaux utilisateurs, administrateurs, téléphonie, imprimante, production, Wi-Fi production, Wi-Fi privé, Wi-Fi public. (Cohen, s.d.)

2.3. Chiffrement des données sensibles

2.3.1. Différents types de chiffrement Chiffrements des données en transit

Dans le cadre des infrastructures sportives modernes, le chiffrement est important pour conserver la confidentialité et l'intégrité des données. Le chiffrement est une technologie fondamentale qui permet d'assurer la protection des données. Les données en transit, au repos ou en cours d'exploitation doivent être chiffrées afin de rester confidentielles. Le chiffrement est le dernier moyen technique de garantir que l'information reste inaccessible pour tout acteur non autorisé. Dans le cadre de l'infrastructure du Clermont-Foot, la plupart des données sont externalisées dans des centres agréés. Ainsi, dans cette situation où les données sont externalisées, assurer un chiffrement robuste devient un prérequis essentiel pour assurer la sécurité des données.

Le chiffrement en transit et au repos est important pour protéger les données externalisées. Ces deux types de chiffrement répondent à différents besoins en termes de cybersécurité.

Le chiffrement en transit vise à sécuriser les données lorsqu'elles circulent sur un réseau, par exemple lors d'un transfert entre l'utilisateur et le serveur, ou entre un client et un prestataire. Il empêche les attaques de type interception ou Man-in-the-Middle, en rendant les informations illisibles à toute personne non autorisée qui tenterait de capter le flux. Cette protection repose généralement sur le protocole Transport Layer Security. Le TLS est un protocole de chiffrement conçu pour sécuriser les communications sur un

réseau informatique. Il est largement utilisé pour sécuriser les connexions entre les navigateurs web et les serveurs en utilisant le protocole HTTPS, ainsi que les courriers électroniques, la messagerie instantanée et les appels VoIP. Ce protocole permet d'établir une session chiffrée en utilisant une combinaison de cryptographie asymétrique pour échanger une clé de session, puis de cryptographie symétrique comme AES pour chiffrer les données échangées.

Le chiffrement au repos, quant à lui, protège les données lorsqu'elles sont stockées sur un serveur ou un dispositif de stockage. Il s'agit de chiffrer les fichiers ou les bases de données avant leur enregistrement sur le support, afin qu'une personne accédant physiquement au disque ou ayant compromis le système ne puisse pas exploiter les informations sans posséder la clé de déchiffrement. Ce type de chiffrement utilise souvent l'algorithme AES, avec des clés de 256 bits pour garantir un haut niveau de sécurité.

La base du chiffrement de bout en bout, est que les données sont chiffrées sur l'appareil de l'utilisateur et ne peuvent être déchiffrées que par le destinataire, personne d'autre. Le chiffrement de bout en bout repose sur un principe fondamental en cybersécurité. Il garantit que seuls les acteurs autorisés, souvent les expéditeurs et les destinataires d'une communication ou les propriétaires des données, puissent accéder au contenu de celles-ci. Son fonctionnement s'appuie principalement sur la cryptographie asymétrique, combinée dans certains cas avec la cryptographie symétrique, afin d'assurer à la fois sécurité et performance.

Lorsque l'utilisateur initie une communication ou dépose des données sur une plateforme utilisant le chiffrement de bout en bout une paire de clés est générée. Il y a une clé publique et une clé privée. La clé publique est partagée librement et permet de chiffrer les données, tandis que la clé privée reste exclusivement en possession de l'utilisateur et est indispensable pour déchiffrer les informations reçues. Le processus débute lorsqu'une donnée est créée ou qu'un message est envoyé, cette information est chiffrée localement sur l'appareil de l'utilisateur à l'aide de la clé publique du destinataire.

Une fois chiffrée, la donnée est transmise sur le réseau jusqu'au serveur du prestataire. Même si une personne malveillante ou le prestataire accède à cette donnée, elle ne pourra pas être interprétée sans posséder la clé privée correspondante. À la réception, le destinataire utilise sa clé privée pour déchiffrer le contenu. L'accès à cette

clé privée est strictement protégé. Elle est souvent stockée dans un coffre-fort logiciel sécurisé sur l'appareil ou protégée par un mot de passe complexe.

Pour renforcer la sécurité et optimiser les performances, le chiffrement de bout en bout emploie fréquemment une combinaison de cryptographie asymétrique et symétrique pour allier sécurité et rapidité. La cryptographie asymétrique est utilisée dans un premier temps pour échanger une clé temporaire appelée clé de session. Cette clé de session est ensuite utilisée avec un algorithme de cryptographie symétrique, pour chiffrer le contenu des communications ou des fichiers. Ce procédé est plus rapide et moins gourmand en ressources que la cryptographie asymétrique seule. Un aspect essentiel du chiffrement de bout en bout est l'authentification des clés publiques. Pour éviter qu'un attaquant n'intercepte la communication et ne substitue sa propre clé publique (attaque de type Man-in-the-Middle), des mécanismes comme la vérification d'empreintes de clés ou l'utilisation de certificats numériques émis par une autorité de confiance sont souvent mis en place.

Il existe des dérivés comme le chiffrement PGP (Pretty Good Privacy) qui repose sur un système de cryptographie asymétrique, fonctionnant sur le même principe que le chiffrement de bout en bout, avec une paire de clés, une clé publique et une clé privée. La clé publique est utilisée pour chiffrer un message ou un fichier, tandis que la clé privée est indispensable pour le déchiffrer. Ce fonctionnement assure que seul le détenteur de la clé privée peut lire les données chiffrées.

Contrairement au chiffrement de bout en bout, qui est généralement intégré de façon transparente dans des applications de messagerie ou de stockage cloud, PGP est principalement utilisé pour la protection des courriers électroniques et des fichiers sensibles. Son usage implique souvent une intervention manuelle pour chiffrer, envoyer, puis déchiffrer les données, ce qui le rend moins fluide que le chiffrement de bout en bout dans des échanges instantanés.

2.3.2. Le chiffrement homomorphique

Le chiffrement de bout en bout permet de garantir la confidentialité des données en empêchant leur lecture par des tiers non autorisés. Cependant, il présente des limites. Il empêche également toute manipulation ou traitement des données chiffrées. Cela signifie qu'une fois les données externalisées, elles ne peuvent être exploitées par le prestataire sans être d'abord déchiffrées, ce qui introduit un risque de compromission.

Le chiffrement homomorphique apparaît comme une avancée majeure en cybersécurité. Contrairement aux méthodes traditionnelles, il permet d'effectuer des calculs directement sur des données chiffrées sans jamais avoir à les déchiffrer. Cela signifie que même un prestataire qui héberge les données de santé des athlètes en exécutant des traitements ne pourra jamais y accéder en clair.

Ce modèle de chiffrement représente une solution clé dans les infrastructures sportives qui n'ont pas de grands systèmes d'information en physique. Grâce au chiffrement homomorphique, il devient possible d'utiliser des services externes sans jamais exposer la confidentialité des données, ce qui constitue une avancée cruciale dans la protection des informations sensibles stockées chez les prestataires.

Le chiffrement homomorphique repose sur un principe mathématique particulier qui autorise l'exécution d'opérations algébriques sur des données chiffrées sans avoir à les déchiffrer. Cette propriété repose sur l'idée que certaines transformations effectuées sur des valeurs chiffrées se répercutent de manière cohérente sur les valeurs en clair correspondantes.

Lorsque des données sont chiffrées à l'aide d'un algorithme homomorphique, chaque donnée en clair est transformée en un chiffre complexe à travers une opération mathématique asymétrique. Ce chiffre est volontairement rendu très volumineux et bruité pour garantir sa confidentialité. Lorsqu'un calcul est effectué sur ces chiffres, le bruit contenu dans les valeurs chiffrées augmente. Cependant, grâce à des techniques spécifiques, il est possible de contrôler ce bruit pour que le déchiffrement final restitue le résultat exact des opérations sur les données initiales.

En pratique, lorsqu'une infrastructure sportive ou une association souhaite déléguer un traitement tout en maintenant la confidentialité, elle chiffre ses données à l'aide de cet algorithme homomorphique. Les données chiffrées sont ensuite envoyées au prestataire, qui applique les opérations demandées directement sur ces valeurs chiffrées. Une fois les calculs achevés, le prestataire renvoie les résultats également chiffrés. L'entreprise, en possession de la clé privée, déchiffre alors le résultat final qui correspond exactement à ce qu'elle aurait obtenu en manipulant les données en clair.

Bien que le chiffrement homomorphique ouvre des perspectives prometteuses pour la protection des données externalisées, il s'accompagne néanmoins de limites importantes qui freinent encore son adoption à grande échelle.

Le chiffrement homomorphique a besoin d'une grande capacité de calcul. Contrairement aux opérations classiques sur des données en clair, chaque addition ou multiplication sur des données chiffrées nécessite des manipulations mathématiques complexes sur de grands nombres. Cela est dû à l'ajout de bruit aléatoire dans les valeurs chiffrées, qui doit être géré tout au long des calculs afin de préserver la confidentialité. Certaines opérations peuvent être jusqu'à 1000 à 1 000 000 de fois plus lentes qu'un calcul équivalent sur des données non chiffrées. Cela rend le chiffrement homomorphique difficilement applicable à des traitements volumineux.

La mise en place de chiffrement homomorphique dans une entreprise requiert du temps et des ressources de calculs adaptées. Les applications standards ne sont pas conçues pour manipuler des données chiffrées de cette manière. Il est donc nécessaire d'utiliser des bibliothèques spécialisées comme Microsoft SEAL ou IBM HELib. Ces outils restent difficiles à maîtriser et requièrent des compétences avancées en cryptographie. Ce facteur risque de freiner les projets car les entreprises devront former les équipes ou bien faire appels à des prestataires externes.

En raison des freins techniques et économiques, le chiffrement homomorphique reste encore peu déployé dans les entreprises et les infrastructures sportives. Il est surtout utilisé dans le cadre de projets pilotes où il y a des exigences de confidentialité. (Matlink, 2015)

2.3.3. Les certificats numériques

Les certificats sont une autre technologie qui permet de vérifier les serveurs vers lesquels les données sont externalisées. Les certificats numériques reposent sur l'utilisation de la cryptographie asymétrique. Lorsqu'un utilisateur souhaite accéder aux informations de santé des athlètes qui sont stockées chez un prestataire externe, le serveur distant présente un certificat numérique qui contient sa clé publique, ainsi que des informations sur son identité (nom de domaine, entreprise, période de validité). Ce certificat est signé numériquement par une autorité de certification, une entité de confiance reconnue, elle-même détenant une clé privée.

Quand le certificat est reçu, l'appareil de l'utilisateur vérifie cette signature en utilisant la clé publique de l'autorité de certification, qui est généralement déjà installée dans les systèmes d'exploitation ou les navigateurs. Si la signature est valide, cela prouve que le certificat n'a pas été falsifié et que l'identité du serveur est authentifiée.

Ensuite, une session sécurisée est établie, en général via le protocole TLS. Lors de cette phase, une clé de session temporaire est générée pour chiffrer les échanges de manière symétrique. Cette clé est elle-même chiffrée avec la clé publique contenue dans le certificat du serveur et transmise à celui-ci, qui est le seul à pouvoir la déchiffrer avec sa clé privée. Une fois cet échange effectué, la communication entre l'utilisateur et le serveur est entièrement chiffrée et authentifiée.

2.3.4. Limites des algorithmes de chiffrements

Les algorithmes de chiffrement qui sont utilisés aujourd'hui, comme RSA ou AES, sont considérés comme sûrs, mais ils présentent tout de même certaines limites qui peuvent poser problème. Ces limites sont principalement liées à la puissance de calcul nécessaire pour garantir la sécurité sur le long terme.

La sécurité des algorithmes asymétriques repose sur des calculs mathématiques complexes, comme la factorisation des grands nombres pour RSA. Les algorithmes symétriques, comme AES, sont quant à eux basés sur des opérations de substitution et de permutation appliquées en plusieurs tours sur les blocs de données. Si AES est aujourd'hui reconnu comme extrêmement robuste, sa sécurité dépend essentiellement de la longueur de sa clé. AES-128 est encore considéré comme sécurisé, mais des organismes comme l'ANSSI recommandent l'usage de clés AES-256 pour des données à protéger sur une longue durée. L'augmentation de la longueur des clés AES renforce la sécurité. Cependant, cela augmente le temps passé sur les traitements et augmente la consommation de ressources.

Une autre menace est actuellement présente, et va devenir importante dans un futur proche. C'est l'arrivée de l'informatique quantique. Pour comprendre facilement la différence entre les ordinateurs quantiques et les ordinateurs classiques, je vais vous présenter l'expérience du chat Schrödinger. Dans cette expérience théorique, un chat est enfermé dans une boîte avec un dispositif pouvant le tuer de manière aléatoire. Tant que l'observateur n'ouvre pas la boîte, le chat est considéré comme à la fois vivant et mort. Ce paradoxe illustre l'état dit de superposition quantique.

De la même manière, les ordinateurs classiques traitent les données sous forme binaire, chaque bit est soit 0, soit 1. En revanche, un ordinateur quantique utilise des qubits, qui peuvent être 0, 1, ou les deux à la fois, tant que l'observation n'a pas lieu. Cette propriété permet à un ordinateur quantique d'effectuer simultanément un grand nombre

de calculs, le rendant potentiellement des millions de fois plus rapide pour certaines opérations complexes.

Les ordinateurs quantiques sont en mesure de réaliser des calculs en quelques heures ou quelques jours. Les ordinateurs classiques prendraient des milliers d'années pour un même calcul. Cela signifierait que toutes les données chiffrées avec RSA pourraient être déchiffrées rapidement, menaçant des années de communications et de stockage soi-disant sûres.

Récemment, une équipe de chercheurs chinois de l'Université de Shanghai a réussi à factoriser une clé RSA de 22 bits en utilisant un ordinateur quantique D-Wave Advantage. Bien que cette taille de clé soit bien inférieure aux standards actuels (2048 bits et plus), cet exploit démontre le potentiel croissant de l'informatique quantique pour remettre en question les systèmes de chiffrement traditionnels. Cette avancée souligne l'importance de développer des algorithmes de cryptographie résistants aux attaques quantiques pour protéger les données sensibles à l'avenir. (Swain, 2024)

Ainsi, si les algorithmes de chiffrement classiques restent essentiels et efficaces aujourd'hui, ils sont soumis à une obsolescence progressive dictée par les avancées technologiques. Une illustration concrète de cette avancée est l'exploit réalisé récemment par une équipe de chercheurs qui a réussi à casser une clé RSA à l'aide d'un ordinateur quantique. Cet exploit démontre néanmoins que la menace est déjà bien réelle et que le développement de machines plus puissantes pourrait remettre en cause la sécurité des standards actuels.

2.4. Mesures spécifiques dans les dispositifs IoT sportifs

Les dispositifs IoT sportifs, tels que les capteurs de performance, les montres connectées et les équipements intelligents utilisés dans les infrastructures sportives, représentent des points d'entrées pour les cyberattaquants. Leur protection repose principalement sur l'installation des mises à jour et des correctifs de sécurité pour se protéger des vulnérabilités. En effet, les cybercriminels exploitent souvent des vulnérabilités logicielles non corrigées pour compromettre ces dispositifs et accéder aux données sensibles des athlètes ou des organisations sportives.

Les mises à jour de firmware permettent de renforcer la sécurité des équipements en corrigeant les vulnérabilités identifiées par les fabricants. Cependant, dans le cadre

des infrastructures sportives, il n'est pas simple de respecter un calendrier de mises à jour régulier pour les équipements. Il y a une grande diversité d'équipements et de fournisseurs. Cela complique l'application de correctifs réguliers. De plus, les mises à jour peuvent provoquer des incompatibilités avec d'autres systèmes en place, nécessitant une phase de tests avant leur déploiement. Pour assurer une gestion efficace des mises à jour, il est crucial de mettre en place des stratégies d'automatisation. L'automatisation réduit les délais d'application des correctifs en intégrant des solutions de gestion centralisée qui surveillent et appliquent les mises à jour en fonction des recommandations des fabricants.

Le cadre réglementaire évolue également pour renforcer la cybersécurité des objets connectés. Au Royaume-Uni, une législation visant à sécuriser les appareils IoT a été introduite afin d'imposer des standards minimaux de protection, notamment l'interdiction des mots de passe par défaut et l'obligation pour les fabricants de publier des mises à jour de sécurité pendant une durée définie après la commercialisation. Ce type de réglementation pourrait influencer les infrastructures sportives en imposant des exigences de conformité en matière de cybersécurité. (GANGLOFF, 2020)

2.5. Endpoint Detection and Response

Un Endpoint Detection and Response (EDR) est une solution de cybersécurité conçue pour surveiller, détecter et répondre aux menaces sur les terminaux d'un réseau. Contrairement aux solutions de protection classiques, l'EDR offre une visibilité approfondie sur l'activité des endpoints (postes de travail, serveurs, objets connectés) et permet une réponse proactive face aux menaces avancées.

Un antivirus repose principalement sur des signatures pour détecter et bloquer les menaces connues. En revanche, un EDR va au-delà de cette approche en surveillant le comportement des endpoints afin de détecter les menaces émergentes et inconnues. Contrairement aux antivirus traditionnels, un EDR permet aussi une réponse active aux incidents, une analyse forensique et une protection contre les techniques avancées utilisées par les cybercriminels. Un EDR fonctionne en collectant et en analysant des données issues des terminaux en temps réel. Il utilise des algorithmes d'intelligence artificielle et d'analyse comportementale pour identifier des activités suspectes. Lorsqu'une menace est détectée, il peut automatiquement isoler l'appareil infecté, bloquer les processus malveillants et alerter les équipes de sécurité. Il s'intègre

généralement avec d'autres outils de cybersécurité pour renforcer la posture globale de défense.

Les infrastructures sportives modernes reposent de plus en plus sur des équipements connectés (IoT, capteurs biométriques, infrastructures de diffusion en direct, réseaux Wi-Fi publics). L'EDR permet d'anticiper et de contrer ces attaques en protégeant les terminaux et en détectant les comportements anormaux avant qu'une compromission ne se propage à l'ensemble du réseau.

J'utilise notamment le Sophos Intercept X avec EDR dans mon entreprise. J'ai fait le choix de sélectionner cette technologie car elle offre une analyse comportementale basée sur l'intelligence artificielle et l'apprentissage automatique pour identifier et neutraliser les menaces en temps réel. Sophos Intercept X offre plusieurs fonctionnalités avancées pour la protection des terminaux. Grâce au Deep Learning, il analyse de manière prédictive les fichiers et comportements afin d'identifier les menaces inconnues avant qu'elles ne compromettent le système. La fonctionnalité Exploit Prevention protège contre les techniques d'attaques avancées, comme l'exécution de code à distance, l'injection de DLL ou encore l'exploitation de failles Zero-Day. Avec Live Response, il permet un accès à distance aux terminaux pour une remédiation rapide en cas d'incident. Enfin, les outils de Threat Hunting facilitent l'investigation en profondeur afin de détecter les menaces persistantes sur l'ensemble du réseau. Cet outil m'a permis plusieurs fois d'analyser certains programmes ainsi que d'empêcher l'exécution de programmes malveillants sur deux postes en 2024.

2.6. Pare-feux et protection des infrastructures sportives

2.6.1. Types de pare-feu

De nos jours, la plupart des systèmes d'information possèdent de nombreux postes informatiques qui sont reliés entre eux par un réseau local. Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et ainsi de travailler en équipe sur des projets communs. Les utilisateurs, les serveurs, les ressources internes doivent parfois accéder au réseau extérieur, c'est-à-dire internet. Le fait d'ouvrir le réseau interne de l'entreprise vers le réseau extérieur peut laisser une porte ouverte aux cyberattaquants.

Pour parer ces intrusions, il est nécessaire d'avoir une architecture réseau sécurisée. Il est important de mettre en place un pare-feu devant l'architecture interne.

Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y remédier au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. De plus, le pare-feu permet aussi de restreindre l'accès interne vers l'extérieur. En effet, des employés peuvent effectuer des activités que l'entreprise ne cautionne pas, comme le partage de fichiers, l'accès à des sites non conformes à sa politique. En plaçant un pare-feu limitant ou interdisant l'accès à ces services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte. Le pare-feu propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau.

Les pare-feux analysent les connexions en tenant compte de leur état et gardent en mémoire les différents attributs de chaque connexion, de leur commencement jusqu'à leur fin, ce qui correspond au stateful inspection. Ils sont capables de traiter les paquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session. L'état NEW correspond à la requête d'un nouvel utilisateur. L'état ESTABLISHED est l'étape après la connexion NEW, c'est pour une connexion déjà initiée. L'état RELATED est peut-être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue. Et enfin, l'état INVALID correspond à un paquet qui n'est pas valide. Ils suivent les connexions du début à la fin et enregistrent des informations comme les adresses IP, les numéros de port et les séquences des paquets. Cette approche permet d'optimiser les performances en appliquant les règles sans relire systématiquement les ACL et d'identifier les paquets anormaux.

Ces pare-feux offrent une bonne protection contre certaines attaques, notamment les attaques DoS comme le SYN Flood, en détectant les tentatives excessives de connexion. Ils permettent également un filtrage plus fin des connexions sortantes en n'autorisant que les réponses légitimes aux requêtes émises. Cependant, ils ne peuvent pas contrôler les protocoles personnalisés non reconnus, nécessitent une réinitialisation des tables d'état lors des modifications de règles et ne protègent pas contre les failles applicatives.

2.6.2. Filtrage du trafic

Le filtrage de paquets sans état (Stateless Packet Filtering) est un système de pare-feu qui fonctionne sur le principe du filtrage simple de paquets. Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine externe. Les en-têtes analysés sont l'adresse IP de la machine

source, l'adresse IP de la machine de destination, le type de paquet (TCP/UDP) et enfin le numéro de port. Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

Le filtrage de paquets avec état ou (State full Packet Filtering) est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et de la couche transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquets. Cela consiste à accorder ou refuser le passage de paquets d'un réseau à un autre en se basant sur l'adresse IP source/destination, le numéro de port source/destination et enfin le protocole de niveaux 3 ou 4 du modèle OSI. Sur la figure 15, j'ai mis en place des règles de filtrage sur le réseau interne. Cela permet à un équipement ou à des équipements appartenant à un VLAN d'accéder à un réseau spécifique.

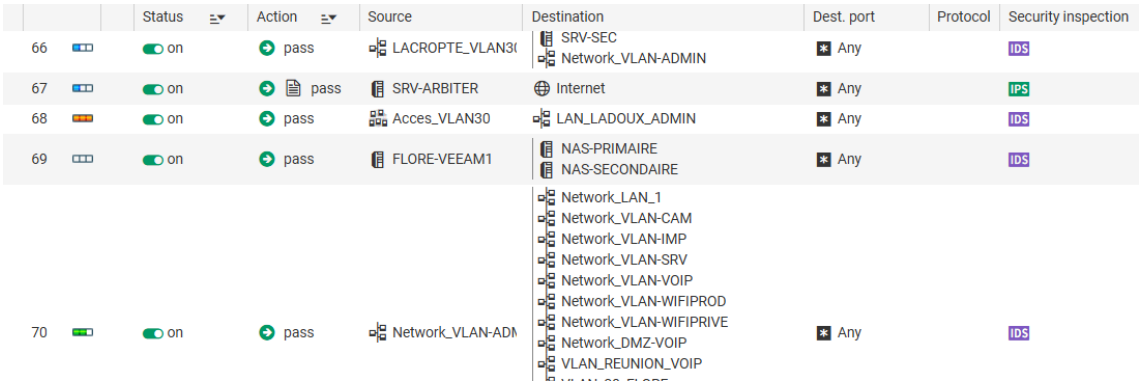

Figure 15, Règle de filtrage, Stateful Packet Filtering

Le filtrage applicatif permet de filtrer les communications application par application. Il opère au niveau de la couche application du modèle OSI, et suppose une connaissance des protocoles utilisés par chaque application sur le réseau, et notamment de la manière dont elles structurent les données échangées. Un pare-feu effectuant un filtrage applicatif est appelé une passerelle applicative ou proxy, car il sert de relais entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et externe, subissant les attaques à leur place.

De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire. Il s'agit d'un dispositif, assurant une bonne protection du réseau, pour peu qu'il soit

correctement administré. En contrepartie, une analyse fine des données applicatives requiert une grande puissance de calcul et se traduit donc souvent par un ralentissement des communications, chaque paquet devant être finement analysé. Par ailleurs, le proxy doit nécessairement être en mesure d'interpréter une vaste gamme de protocoles et de connaître les failles pour être efficace. Sur la figure 16, j'ai mis en place des règles de filtrage qui autorisent le trafic du réseau interne vers internet, mais en sélectionnant des web services associés à du Anydesk, TeamViewver, Datto RMM, Microsoft ou Google.

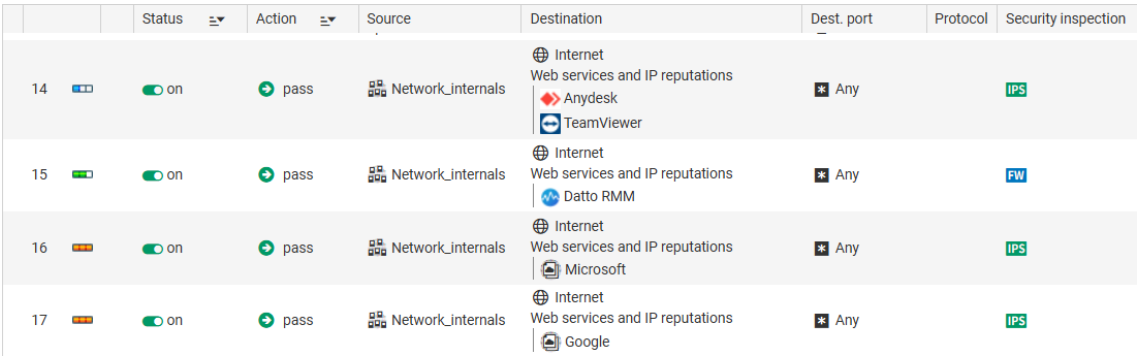

Figure 16, Règle de filtrage applicatif

L'URL filtering sur Stormshield permet de contrôler l'accès aux sites web en les classant par catégories, comme les sites académiques, d'entreprise ou illégaux. Je définis les règles pour autoriser ou bloquer l'accès selon les catégories, ce qui renforce la sécurité et la gestion de la navigation. Cette fonctionnalité empêche l'accès aux sites malveillants, limite les distractions en entreprise et aide à respecter les politiques de conformité. Elle repose sur une base de données régulièrement mise à jour pour une protection efficace. L'interface permet aussi d'ajouter des règles personnalisées pour affiner le filtrage selon les besoins spécifiques. Sur la figure 17, j'ai bloqué notamment les sites illégaux, les sites pornographiques, les sites de paris, les sites d'armes, les sites de drogue. La catégorisation des sites sur Stormshield repose sur une base de données interne. Elle est ensuite enrichie par des fournisseurs tiers et des technologies d'analyse en temps réel. Le moteur de filtrage évalue les sites en fonction de leur contenu et de leur risque, en utilisant des algorithmes d'intelligence artificielle et de sandboxing. (Monmarché, 2023)

Status	Action	URL category	Comments
on	Pass	bank	
on	Pass	business	
on	Pass	employment	
on	Pass	entertainment	
on	Block	illegal	
on	Pass	it	
on	Pass	news	
on	Pass	online	
on	Block	pornography	

Figure 17, URL Filtering Stormshield

2.6.3. Web Application Firewall (WAF)

Les modèles de sécurité actuels recommandent le déploiement en front d'un Web Application Firewall (WAF). Un WAF est conçu pour protéger les applications Web en filtrant, surveillant et bloquant tout trafic HTTP entrant malveillant, tout en empêchant les données non autorisées de quitter l'application. Sur la figure 18, le WAF est placé entre l'utilisateur et le serveur web, où il filtre le trafic HTTP/S. Selon son paramétrage, il analyse toutes les requêtes provenant du trafic internet, en laissant passer les requêtes légitimes et en interceptant les requêtes malveillantes. Ainsi, il limite les attaques exploitant les failles de sécurité de toute l'infrastructure web. Le WAF fonctionne comme un proxy inversé.

Figure 18, Fonctionnement d'un WAF

Le pare-feu est conçu pour arrêter les menaces visant les applications web. Il permet notamment de stopper les attaques par injection SQL, les attaques DDoS, les attaques XSS, les attaques par force brute, les attaques par contrebande de requêtes HTTP, le détournement de clic et bien d'autres.

Un WAF permet également de surveiller en continu le trafic web afin d'identifier des comportements anormaux et d'alerter les administrateurs en cas de tentative d'intrusion. Les solutions avancées proposent des tableaux de bord permettant de visualiser en temps réel les tentatives d'attaques, leur origine et leur nature. Ces données permettent d'affiner les règles de filtrage et de renforcer la posture de sécurité des applications web.

J'ai notamment eu l'opportunité de réaliser un audit externe sur le site web de mon Club de Badminton. Cela m'a permis de tester mes compétences dans un cadre associatif. Après avoir mis en place les accords par écrit avec le président du club, j'ai pu auditer le site web https://cbc63.fr/

J'ai commencé par vérifier les ports ouverts sur le site web, et les services associés derrière chaque port. J'ai pu détecter un serveur Apache. J'ai pu examiner ce serveur afin de vérifier la configuration. Il n'y a aucun fichier de configuration, de fichiers sensibles, de sauvegarde accessible publiquement. La version du serveur Apache est à jour. Il n'y a pas de vulnérabilité connue sur cette version à ce jour.

J'ai ensuite vérifié si les données sensibles étaient bien protégées. Les communications entre le client et le serveur doivent être sécurisées à l'aide du protocole HTTPS et des versions récentes de TLS. Il y a bien un certificat HTTPS d'une durée de validité de 1 an, renouvelé en mai par Let's Encrypt. Les communications entre le client et le serveur sont chiffrées via le protocole TLS. La négociation de la version se fait seulement avec la version 1.2 et 1.3, ce qui est une bonne chose en matière de sécurité puisqu'il n'accepte pas 1.1 et 1.0.

J'ai vérifié s'il était possible d'accéder à des informations sensibles à travers des erreurs de debug ou des en-têtes HTTP mal configurés. Il est malheureusement possible d'accéder à des informations sensibles puisque le CSP n'est pas configuré. La politique de sécurité du contenu (CSP) est une couche de sécurité supplémentaire qui permet de détecter et d'atténuer certains types d'attaques. Ces attaques sont utilisées pour tout, du vol de données à la dégradation de sites ou à la distribution de logiciels malveillants. CSP fournit un ensemble d'en-têtes HTTP standard qui permettent aux propriétaires de sites Web de déclarer les sources de contenu approuvées que les navigateurs devraient être autorisés à charger sur cette page. Cela permet donc de limiter les attaques de type Cross Site Scripting (XSS) et par injection de données.

J'ai ensuite vérifié s'il y avait la présence de Sender Policy Framework et de Domain-based Message Authentication, Reporting, and Conformance. Le SPF est un protocole d'authentification des emails qui permet de définir une liste de serveurs autorisés à envoyer des emails au nom d'un domaine. Il aide à prévenir le spoofing et le phishing en permettant aux serveurs de messagerie destinataires de vérifier si l'email provient bien d'une source légitime. Sur la figure 19, j'ai vérifié la présence de l'inscription SPF.

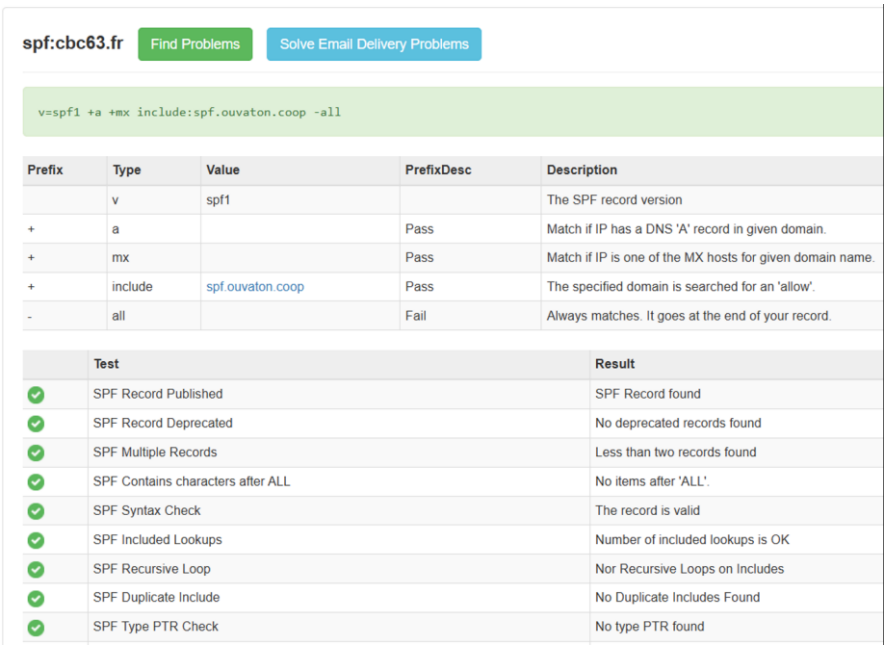

Figure 19, Présence du SPF sur le site cbc63.fr

Le DMARC est un protocole d'authentification des emails qui s'appuie sur SPF et DKIM pour prévenir le spoofing et le phishing. Il permet aux propriétaires de domaines de définir une politique sur la manière dont les emails non authentifiés doivent être traités (none, quarantine, reject) et fournit des rapports détaillés sur les tentatives d'usurpation d'identité. Sans DMARC, un attaquant peut toujours falsifier l'expéditeur d'un email, même si SPF et DKIM sont configurés. Cependant, il n'y a pas de DMARC actuellement configuré sur le site web. Je leur ai donc recommandé de contacter leur prestataire web.

J'ai terminé mon audit en vérifiant les fuites de données. J'ai récupéré les mails internes des collaborateurs. Puis, j'ai regardé si des couples emails/logins et mots de passe avaient fuité. J'ai utilisé les plateformes de leak-look-up et haveibeenpwned.

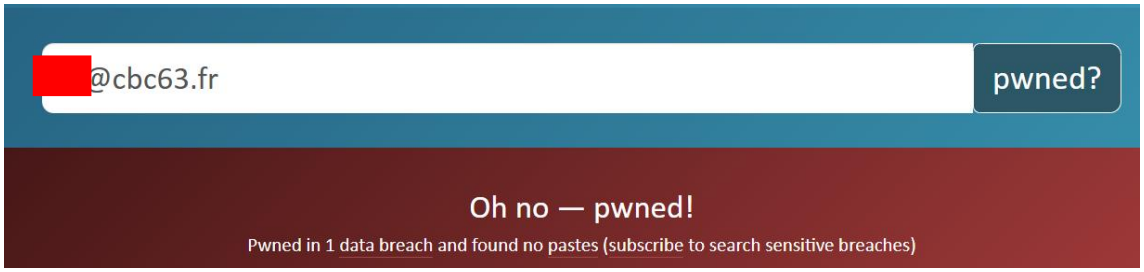

Figure 20, Fuites de données cbc63.fr

Les remédiations sont surtout pour le développeur et l'hébergeur du site web pour mettre en place le DMARC et les en-têtes CSP. Pour les utilisateurs, je leur ai recommandés de changer leurs mots de passe.

3. Protocole en cas d'attaque

3.1. Plans de reprise d'activité (PRA) et de continuité (PCA)

Le plan de continuité d'activité et le plan de reprise d'activité sont des plans qui vont intervenir pendant et après une attaque pour garantir la résilience face aux cyberattaques.

Le PCA vise à maintenir un niveau de service minimum en cas d'incident grave. Il permet d'assurer le fonctionnement des infrastructures critiques, comme les systèmes de billetterie, la gestion des accès aux stades ou la diffusion en streaming des événements. L'objectif est d'éviter une interruption totale des services et de garantir une expérience utilisateur fluide, malgré l'incident en cours.

Le PRA est activé une fois que l'incident est maîtrisé et permet de restaurer l'ensemble des services impactés pour revenir à un état normal. Il inclut la restauration des systèmes à partir de sauvegardes hors site, le redémarrage des infrastructures critiques, la mise en œuvre des actions correctives pour éviter que l'attaque ne se reproduise et l'ordre de remise en route des différents services.

Imaginons une attaque par rançongiciel sur les serveurs informatiques d'un stade accueillant un match de foot de Ligue 1. Pendant la mi-temps, un message s'affiche sur les écrans internes indiquant que les données du système de billetterie, de gestion des accès et des caméras de surveillance sont chiffrées, avec une demande de rançon en échange de leur restitution. Les conséquences immédiates sont les suivantes. L'incapacité à valider les billets à l'entrée du stade, ce qui perturbe la gestion des flux de spectateurs. L'impossibilité pour le personnel de sécurité d'accéder aux images de

vidéosurveillance, augmentant ainsi les risques d'incidents. Un arrêt temporaire du système de paiement des boutiques et des fast-foods.

Dans cette situation, l'activation du PCA permettrait de basculer sur des solutions de secours, comme un système manuel de contrôle des billets, une surveillance humaine accrue et une reprise temporaire du paiement en espèces. Une fois le rançongiciel neutralisé, le PRA interviendra pour restaurer les systèmes dans l'ordre (sécurité, puis billetterie, puis encaissement) à partir de sauvegardes sécurisées et analysera l'attaque afin d'appliquer des correctifs.

Au sein du Clermont-Foot, lorsqu'il y a un incident informatique. La DSI recommande de déconnecter tous les utilisateurs du réseau interne afin de ralentir la propagation de la menace et de l'isoler. Ensuite, ils mettent en place une cellule de crise, prennent contact avec leur prestataire de maintien en condition opérationnelle et maintien en condition de sécurité. Et enfin, ils activent le plan de continuité d'activité pour que les collaborateurs puissent travailler. Une fois la menace gérée, ils remettent en place le système d'information grâce aux sauvegardes en suivant le plan de reprise d'activité.

3.2. Gestion de crise et communication avec les parties prenantes

La gestion de crise cyber dans les infrastructures sportives repose sur une communication efficace et structurée. Dans ce secteur, la réputation et la continuité des événements est primordiale. Il est important de pouvoir réagir rapidement et correctement afin de garantir la transparence vis-à-vis du public et de la retransmission lors d'une crise.

Lorsqu'un incident survient, l'activation immédiate d'une cellule de crise permet de structurer la réponse à l'attaque. Cette cellule doit regrouper des responsables des systèmes d'information, des experts en cybersécurité, des juristes, des communicants et des représentants de la direction. Le but de cette cellule est de coordonner les actions techniques et décisionnelles tout en gérant la communication interne et externe.

La communication de crise cyber repose sur des principes fondamentaux. L'anticipation est un élément clé qui passe par la préparation de scénarios d'incidents, intégrant différents niveaux de gravité et leurs impacts potentiels. Un plan de

communication de crise doit être défini en amont (communiqués de presse, réseaux sociaux, notifications internes). L'ANSSI recommande la mise en place d'une boîte à outils de communication cyber, contenant des réponses types pour différents types d'attaques (rançongiciel, DDoS, fuite de données).

Lors de la gestion active de l'incident, la posture de communication peut être de deux types. Elle peut être proactive, en communiquant rapidement sur la situation pour rassurer et démontrer une gestion efficace de la crise, ou réactive, en contrôlant les informations diffusées pour éviter toute panique ou exploitation malveillante de la situation. La vulgarisation des aspects techniques est importante afin de permettre au public et aux médias de comprendre la nature et l'impact de l'attaque.

L'identification des acteurs de la communication permet de définir un porte-parole officiel. Cette personne va centraliser les informations et gérer la communication avec les prestataires externes (ANSSI, prestataires, cabinets de gestion de crise) et les personnes internes (employés, sportifs).

La dernière étape est la phase de retour d'expérience (RETEX) lorsque la crise est maîtrisée. Le but est d'analyser la gestion de l'incident afin d'apporter des améliorations pour les futures menaces.

IV. Étude de cas des JO 2024

1. Complexité de la cybersécurité lors des JO 2024

1.1. Coordination entre les parties prenantes

La première difficulté réside dans la coordination de l'ensemble des parties prenantes en cybersécurité. En France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a piloté la stratégie de cybersécurité des Jeux en lien étroit avec le gouvernement et le Comité d'organisation des JO (COJOP). Cette préparation a mobilisé différents acteurs tels que l'État, l'organisation des Jeux, les réseaux CSIRT, les partenaires internationaux. L'enjeu était d'unifier les efforts de tous ces acteurs au sein d'un dispositif cohérent. Une cellule cyber dédiée a été mise en place au sein du centre des opérations technologiques des JO. Cette cellule a rassemblé les experts en cybersécurité d'Eviden (filiale d'Atos), le principal prestataire IT des Jeux, ceux du COJOP et du Comité International Olympique, ainsi que des représentants de l'ANSSI, le tout en lien avec d'autres partenaires comme les opérateurs de réseaux Orange ou Cisco. Plus de 100 experts se sont relayés en permanence dans ce Cyber Security Operations Center (CSOC) réparti sur trois sites en Europe pour surveiller et répondre aux incidents éventuels.

Cette approche collaborative et centralisée visait à détecter rapidement toute menace et à coordonner la réponse entre les différentes entités. Au-delà des équipes dédiées, l'ANSSI a également intégré le secteur privé plus largement dans l'effort de sécurité. De grandes entreprises françaises de cybersécurité comme Thales, Orange Cyberdéfense, Atos ou Stormshield ont apporté leurs solutions et expertises, tandis que des fournisseurs cloud tels qu'AWS ou OVHcloud ont été mis à contribution pour l'hébergement sécurisé de certaines applications olympiques. De même, les opérateurs télécom ont joué un rôle clé pour assurer la résilience des réseaux de communication mobilisés pendant l'événement. La coopération s'est étendue à l'international avec le soutien d'organismes comme l'ENISA (agence européenne) ou la CISA américaine, afin de partager des renseignements sur les menaces et les bonnes pratiques à adopter. Cette alliance public-privé à grande échelle a été perçue comme essentielle pour garantir la cybersécurité des Jeux.

Enfin, un important travail de sensibilisation et de formation a été mené auprès des diverses parties prenantes. Un plan de sensibilisation a bénéficié à plusieurs centaines d'acteurs impliqués dans l'organisation, pour renforcer leur niveau de

vigilance et d'hygiène informatique face aux menaces. Des exercices de simulation et de gestion de crise cyber ont également été organisés par l'ANSSI à destination des opérateurs critiques des Jeux, afin de tester et d'améliorer leur réaction en cas d'incident majeur. Grâce à cette coordination sans précédent entre tous les acteurs (autorités étatiques, partenaires technologiques, opérateurs et communautés CERT) les JO de Paris ont abordé l'échéance avec un front uni en cybersécurité.

1.2. Infrastructures temporaires et systèmes décentralisés

La seconde source de complexité tenait à la nature des systèmes informatiques des Jeux, à la fois temporaires et décentralisés. La tenue d'un événement sportif de cette ampleur requiert en effet de déployer un très grand nombre de systèmes d'information sur une période réduite. Bon nombre de ces infrastructures numériques ont été créées spécifiquement pour l'occasion, pour équiper des sites de compétition éphémères ou des besoins inédits, puis ont été démantelées une fois les Jeux terminés. Par ailleurs, ces systèmes sont hautement interconnectés entre eux et répartis sur des dizaines de sites différents à travers le pays (stades, arènes, centres médias, etc.). Chaque site, chaque application peut être opérée par des prestataires ou équipes différentes, avec des niveaux de sécurité et de maturité identiques. Comme l'a averti l'ANSSI, de tels événements nécessitant la mise en place de nombreux SI par une multitude d'acteurs aux niveaux de sécurité variables offrent aux attaquants une surface d'exposition élargie.

En effet, la coexistence de tant de systèmes décentralisés rend l'ensemble potentiellement vulnérable au maillon le plus faible. Une simple faille sur une infrastructure temporaire moins bien protégée pourrait servir de porte d'entrée à une attaque plus large. Les attaquants peuvent profiter de ce contexte pour surveiller ou extorquer les organisateurs et participants, et exploiter la forte médiatisation afin de ternir l'image du pays hôte ou perturber le déroulement de l'événement.

La décentralisation implique qu'aucune entité unique ne contrôle l'ensemble des composants. La sécurité dépend donc de la confiance et de la conformité de chaque acteur tiers (fournisseurs, sous-traitants, sponsors techniques, etc.). Pour Paris 2024, il a fallu mettre en place une gouvernance capable de superviser cet écosystème fragmenté. L'ANSSI et le COJOP ont ainsi dû édicter des protocoles de sécurité communs, des normes minimales à respecter partout, et veiller à leur bonne application sur le terrain. Malgré la complexité de ce tissu informatique décentralisé, cette approche visait à

réduire les angles morts et à empêcher qu'un système isolé ne devienne la cible idéale des attaquants.

2. Menaces spécifiques ciblant les JO 2024

2.1. Cyberattaques politiques

Les Jeux Olympiques constituent une tribune mondiale qui est au centre des enjeux politiques et idéologiques. Il n'est donc pas étonnant que des attaques d'origine politique aient figuré parmi les menaces redoutées. Des groupes sponsorisés par des États (appelés APT pour Advanced Persistent Threats) peuvent chercher à exploiter les JO pour servir leurs intérêts géopolitiques. D'autre part, des hacktivistes motivés par une cause pourraient viser l'événement pour faire passer un message ou dénoncer une situation. Ces acteurs étatiques ou activistes peuvent avoir pour objectif de déstabiliser l'organisation des Jeux, de discréditer le pays hôte sur la scène internationale, voire de perturber les épreuves sportives elles-mêmes. La visibilité immense des JO amplifie en effet l'impact potentiel de telles opérations.

Par exemple, une cyberattaque qui ferait scandale pendant les Jeux entacherait gravement la réputation de la France, ce que recherchent certains adversaires idéologiques. L'ANSSI soulignait en amont que les attaquants ne manqueraient pas « d'exploiter les tensions géopolitiques » entourant la France en 2024. ((ANSSI), 2024) Le contexte international était effectivement marqué par la guerre en Ukraine et d'autres frictions, alimentant le risque de voir des campagnes d'espionnage ou de dénigrement ciblées contre les JO. L'histoire récente a montré que ce risque est bien réel. Lors des JO d'hiver de 2018 à PyeongChang, une attaque informatique d'ampleur menée lors de la cérémonie d'ouverture des Jeux a cherché à saboter l'événement. De même, à l'approche des JO de Tokyo 2020, des opérations d'espionnage ont été détectées contre le comité d'organisation, impliquant un groupe lié au renseignement militaire russe (Sandworm) infiltrant les réseaux pour y collecter des informations sensibles.

Ce type d'APT, agissant pour le compte d'un État, aurait pu viser en 2024 viser à la fois les systèmes des Jeux (pour voler des données ou préparer un sabotage) et les partenaires ou sponsors liés à des nations rivales. Par ailleurs, des collectifs hacktivistes ont pu menacer de défacer des sites web officiels ou de divulguer des données en soutien à des causes (écologie, droits humains, etc.), profitant de l'audience médiatique des JO. La menace dite politique englobait aussi bien l'espionnage discret que le cybersabotage revendiqué, tous deux pouvant troubler le bon déroulement ou l'image des Jeux. Paris

2024 a donc dû se préparer à contrer des adversaires déterminés et sophistiqués, capables de mobiliser des ressources importantes pour atteindre leurs buts idéologiques.

2.2. Perturbations des systèmes critiques

Au-delà des attaques motivées par la politique, un scénario redouté était la perturbation des systèmes critiques supportant l'événement. Les JO s'appuient sur un ensemble de services numériques et d'infrastructures dont le bon fonctionnement est crucial pour le déroulement des compétitions et l'expérience des spectateurs (systèmes de billetterie et de contrôle d'accès, réseaux de transport, alimentation énergétique des sites, systèmes de chronométrage et de diffusion médiatique des épreuves, etc). Une attaque sur l'un de ces systèmes pourrait provoquer le chaos logistique ou même interrompre les Jeux.

Ce risque n'était pas seulement théorique, il s'est déjà matérialisé par le passé. Lors des JO de Londres en 2012, les équipes de cybersécurité ont recensé un total de 212 millions de cyberattaques durant l'événement, dont une tentative notable de déni de service (DDoS) visant l'infrastructure électrique du parc olympique. Si cette attaque n'a pas causé de panne majeure, elle a révélé la vulnérabilité potentielle des réseaux d'énergie. Mais l'exemple le plus marquant reste celui de PyeongChang 2018. La cérémonie d'ouverture des Jeux sud-coréens a subi une attaque informatique coordonnée qui a mis hors service plusieurs systèmes critiques. L'Olympic Destroyer a provoqué l'interruption du site web officiel et des services en ligne des JO, empêchant de nombreux spectateurs d'imprimer leurs billets d'entrée, a paralysé le Wi-Fi dans le stade, et a même causé des pannes d'écrans d'affichage et un dysfonctionnement des portes d'accès électroniques. En pleine cérémonie d'ouverture, ces perturbations ont semé la confusion et montré à quel point une intrusion numérique pouvait avoir des effets concrets sur le terrain. (CTI-TEAM, 2024)

Avec Paris 2024, de telles perturbations figuraient parmi les craintes principales. Une attaque sur le système de billetterie aurait pu, par exemple, bloquer l'accès du public aux sites de compétition, engendrant des foules aux entrées et des problèmes de sécurité physique. De même, un sabotage des feux de circulation ou du réseau ferroviaire d'Île-de-France aurait perturbé le transport de milliers de spectateurs et d'athlètes, risquant des retards ou des annulations d'épreuves. Une intrusion dans les systèmes des médias ou dans le signal international de diffusion télévisée aurait eu un retentissement planétaire, coupant potentiellement la transmission en direct de finales attendues.

En 2024, les organisateurs ont tout mis en œuvre pour éviter le scénario du « coup de froid numérique » sur les Jeux; Ils ont multiplié les sauvegardes pour les services critiques, les plans de secours manuels (par exemple des listes imprimées de billets en dernier recours), la redondance des réseaux et simulations régulières de panne afin de tester la résilience. Malgré ces précautions, entre le 8 mai (arrivée de la flamme à Marseille) et le 8 septembre 2024, l'ANSSI a recensé pas moins de 548 événements de cybersécurité touchant des entités liées aux JO. Parmi eux, 83 incidents ont été qualifiés de graves, mais aucune perturbation réelle des Jeux n'a eu lieu. Cela signifie que toutes les tentatives pour désorganiser les systèmes critiques ont pu être contenues ou neutralisées à temps. Ce succès inédit souligne l'efficacité des mesures de protection déployées pour Paris 2024. (DILKOFF, 2024)

2.3. Rançongiciels et sabotage technologique

Une troisième catégorie de menaces regroupait les attaques à but criminel ou de sabotage technologique, en particulier via des rançongiciels ou l'exploitation d'objets connectés et de dispositifs numériques présents autour des Jeux. Les rançongiciels constituent l'une des menaces cyber les plus répandues ces dernières années, et les JO n'y échappaient pas. Des groupes cybercriminels opportunistes pouvaient tenter de s'introduire dans les réseaux olympiques ou ceux de leurs fournisseurs pour y déployer un malware de chiffrement, puis exiger une rançon en échange de la restauration des données. L'ANSSI notait que les groupes de rançongiciel « ratissent au plus large » et n'hésitent plus à s'en prendre à tout type d'organisation, des grandes entreprises aux PME en passant par les collectivités et même les associations. L'écosystème des JO comprend de nombreux partenaires et prestataires de taille modeste (sous-traitants techniques, fédérations sportives, fournisseurs locaux, etc.) qui peuvent se croire à tort à l'abri de la menace. En réalité, ces petites structures sont des cibles de choix du fait de leurs moyens de sécurité limités.

Si un rançongiciel venait à en compromettre plusieurs simultanément, les attaquants pourraient créer un effet de masse pour faire parler d'eux médiatiquement et ternir l'image de l'organisation, même si les systèmes centraux des JO ne sont pas touchés. Par exemple, l'infection de la société gérant les accréditations ou d'un transporteur de matériel sportif paralyserait indirectement une partie de l'événement tout en exposant les données sensibles. C'est pourquoi les autorités ont insisté pour que tous les acteurs, grands et petits, liés aux Jeux renforcent leurs défenses, en particulier contre le phishing qui est le vecteur privilégié des rançongiciels.

En parallèle, la notion de sabotage technologique recouvre des actions malveillantes exploitant des objets physiques connectés ou des systèmes technologiques de pointe pour nuire au bon déroulement des JO. Les drones peuvent transporter des charges dangereuses, filmer des zones sensibles ou brouiller des communications. La menace de drones malveillants était prise très au sérieux pour Paris 2024, au point que des unités spécialisées de lutte anti-drone ont été déployées pour l'occasion. Un drone pourrait par exemple survoler un site de compétition en violant la zone d'exclusion aérienne, forçant l'interruption d'une épreuve, ou servir de relais improvisé pour tenter une intrusion dans les réseaux sans fil d'un stade. Les objets connectés élargissent la surface de menace. Les capteurs intelligents qui gèrent la température, la lumière, des badgeuses et tourniquets connectés contrôlent l'accès des milliers de bénévoles et officiels, les appareils électroniques que portent ou utilisent les participants (montres connectées, tablettes, systèmes de chronométrage sportifs, etc.). Chacun de ces points d'entrée potentiels pourrait, s'il était compromis, servir à un sabotage. (Gatewatcher, s.d.)

Même sans piratage sophistiqué, des actes de malveillance physique comme le sabotage de câbles télécom entrent dans ce registre de menaces hybrides mêlant cyber et physique. Face à ces risques, les organisateurs des JO 2024 ont déployé un éventail de mesures préventives. D'une part, une surveillance renforcée des réseaux a été assurée pour détecter toute activité suspecte pouvant indiquer la présence d'un rançongiciel avant son activation. D'autre part, une attention particulière a été portée à la sécurité des objets connectés déployés sur les sites. Les équipes de cybersécurité effectuent des tests de pénétration sur les dispositifs IoT critiques, un filtrage strict des appareils autorisés, un chiffrement des communications des capteurs sensibles.

3. Rôle des acteurs majeurs dans la cybersécurité des JO 2024

3.1. Contribution de l'ANSSI

En tant qu'autorité nationale, l'ANSSI a eu un rôle central de coordination et d'expertise pour Paris 2024. Chargée par le gouvernement de piloter la stratégie cybersécurité des Jeux, l'agence a défini une feuille de route dont l'objectif ultime était qu'aucune cyberattaque ne perturbe significativement l'événement. Pour atteindre ce but, l'ANSSI a déployé une démarche en plusieurs volets. D'abord, elle a travaillé en amont à l'évaluation de la menace. S'appuyant sur les retours d'expérience des précédents JO et d'autres grands événements sportifs, ses équipes de renseignement et

d'anticipation (CERT-FR) ont identifié les scénarios d'attaque les plus plausibles et les systèmes les plus à risque. Un rapport publié en 2023 a synthétisé les principales menaces pesant sur les JO 2024 et formulé des recommandations sectorielles.

Ce travail a permis de sensibiliser tous les acteurs impliqués aux dangers spécifiques (espionnage, sabotage, rançongiciel, etc.) et d'orienter les investissements de sécurité là où ils étaient le plus nécessaires. Ensuite, l'ANSSI a élaboré et diffusé des protocoles de sécurité et de bonnes pratiques à destination des organisations participant aux Jeux. Cela a couvert des mesures techniques (configuration sécurisée des systèmes, segmentation des réseaux, sauvegardes régulières, détection d'intrusions…) mais aussi des procédures à suivre en cas d'incident. L'agence a conseillé le COJOP et les partenaires sur le durcissement des infrastructures critiques identifiées. Elle a publié des guides de recommandations et a veillé à leur appropriation par les différentes équipes IT des Jeux. En parallèle, l'ANSSI a mené une campagne de sensibilisation de grande ampleur pour élever le niveau de vigilance de tous les intervenants, y compris non techniques. Des centaines de personnes (organisateurs, bénévoles, prestataires) ont été formées aux principes de base de l'hygiène numérique afin de réduire le risque d'erreur humaine (phishing, utilisation de mots de passe faibles, etc.). Par ailleurs, l'ANSSI a joué un rôle de facilitateur opérationnel pendant l'événement. Elle a collaboré étroitement avec les équipes du COJOP, le CIO et les prestataires cyber (comme Eviden, Atos) pour assurer une réponse unifiée face aux incidents.

Intégrée au CSOC olympique, l'ANSSI a pu faire le lien avec les autres secteurs critiques nationaux. Si une menace dépassait le cadre strict des Jeux, l'ANSSI pouvait mobiliser les moyens nationaux (par exemple le centre gouvernemental de crise cyber) et coordonner l'intervention avec les forces de l'ordre. Cette posture proactive a garanti qu'aucun incident ne reste isolé. Toute alerte locale pouvait être rapidement escaladée au niveau national si nécessaire, et inversement les renseignements nationaux sur des campagnes en cours étaient partagés avec les défenseurs des JO.

Enfin, l'ANSSI a cultivé la coopération internationale autour de la cybersécurité de Paris 2024. Consciente que les menaces olympiques sont globales, elle a échangé avec ses homologues étrangers pour partager des informations et parer aux attaques transfrontalières. Un partenariat étroit avec le BSI allemand qui préparait la sécurité de l'Euro de football 2024, a permis un retour d'expérience mutuel. Les deux agences ont

d'ailleurs publié conjointement un rapport mettant en lumière l'importance de la collaboration public-privé dans la sécurisation des grands événements sportifs.

De même, l'ANSSI a bénéficié des retours du NCSC britannique (hôte des JO 2012) et a travaillé avec le réseau européen des CERT pour surveiller toute activité suspecte liée aux Jeux au-delà des frontières. Cette dimension internationale a enrichi l'arsenal de défense de Paris 2024 et posé les bases d'une solidarité cyber pour les grandes manifestations à venir. L'ANSSI a grandement contribué à ce que les JO de Paris 2024 se déroulent sans incident cyber majeur. Elle a en quelque sorte agi comme le chef d'orchestre discret assurant l'harmonie de l'écosystème de cybersécurité déployé autour de l'événement. Développement de protocoles de sécurité, recommandations techniques et bonnes pratiques à adopter par les organisations impliquées.

3.2. Solutions déployées pour Paris 2024

Pour contrer les menaces multiples évoquées, un ensemble de solutions de cybersécurité ont été déployées autour des JO 2024, combinant moyens humains, procédés organisationnels et technologies de pointe. Au cœur du dispositif, il y a les centres opérationnels de sécurité (SOC) dédiés aux Jeux. Le principal CSOC, opéré par les équipes d'Eviden/Atos en coordination avec l'ANSSI, a fonctionné 24h/24 pendant toute la durée de l'événement. Il s'appuyait sur des relais en Europe pour assurer une redondance. Ces centres de supervision ont agrégé en temps réel les journaux d'événements de sécurité provenant de milliers d'équipements (serveurs, pare-feu, applications, etc.) déployés sur les sites olympiques. Des analystes SOC expérimentés scrutaient ces flux à la recherche du moindre signe d'intrusion ou d'anomalie. Dès qu'une activité suspecte était détectée (tentative de connexion anormale, mouvement latéral dans le réseau, etc.), une procédure d'alerte et d'escalade rapide permettait d'enquêter et de répondre avant que l'incident ne prenne de l'ampleur. (MARCOU, 2024)

Sur le plan technologique, une panoplie d'outils de sécurité avancés a été utilisée. Des systèmes de détection/prévention d'intrusion (IDS/IPS) étaient déployés sur le réseau olympique pour identifier les attaques connues (signatures de malware, patterns de scans ou de DDoS) et bloquer instantanément celles-ci. Des sondes de détection type SIEM couplées à des solutions d'analyse comportementale surveillaient en profondeur les activités afin de repérer d'éventuelles menaces inédites passant sous le radar des filtres classiques. Par ailleurs, un important dispositif de Threat Intelligence a été mis en place. Les renseignements sur les menaces collectées en amont (adresses IP

malveillantes, indicateurs de compromission, alertes internationales) ont été injectés dans les outils afin de disposer de listes noires et de scénarios de détection calibrés sur la menace réelle pesant sur les Jeux. Cette veille a été enrichie tout au long de l'événement par le partage d'informations entre partenaires.

L'intelligence artificielle (IA) a également fait son apparition parmi les armes défensives. Compte tenu du volume gigantesque de données de sécurité à analyser, des algorithmes d'apprentissage automatique ont été déployés pour aider à distinguer le bruit de fond des signaux réellement inquiétants. L'IA a servi par exemple à établir une ligne de base du comportement normal des systèmes et à alerter sur des écarts significatifs pouvant trahir une attaque sournoise. Elle a aussi été utilisée pour corréler entre eux des événements dispersés mais liés. L'intégration de l'IA visait à améliorer la détection proactive des menaces et la réactivité des défenses. Néanmoins, ces outils automatisés ont été employés en soutien des analystes humains, qui gardèrent la décision finale "l'IA ne remplace pas l'expertise, mais l'augmente dans ce contexte".

En plus de la détection, des mesures concrètes ont été prises pour protéger activement les systèmes. Le cloisonnement des réseaux a été affiné, des mécanismes de redondance et de sauvegarde robustes ont été mis en place pour assurer la continuité des services même en cas d'incident, et des tests de pénétration réguliers ont été menés en amont pour éprouver les défenses et combler les failles identifiées. Notamment, dans les mois précédant les Jeux, les équipes cyber ont simulé divers scénarios d'attaques (intrusion externe, complice interne malveillant, sabotage physique couplé à du hacking) afin de tester la coordination entre les acteurs et la robustesse des procédures.

Lorsque les Jeux ont débuté, l'ensemble des solutions techniques comme organisationnelles était en place et rodé. Les centres de sécurité étaient en alerte maximale. Les outils de détection sont affûtés. Le personnel est entraîné à réagir vite. Ce maillage défensif dense explique en grande partie pourquoi aucune attaque n'a réussi à causer de dégâts pendant l'événement. (Les Jeux Olympiques 2024 : Un grand événement sportif où des enjeux sûreté, cybersécurité et réputations se superposent, 2021)

3.3. Préparation pour les futures menaces

L'expérience de Paris 2024 en matière de cybersécurité constitue désormais une référence pour les grandes manifestations à venir. Les leçons apprises durant cet

événement vont permettre d'améliorer les stratégies de défense et de standardiser les pratiques efficaces. Premièrement, le fait d'avoir empêché toute perturbation cyber majeure pendant les Jeux est une première historique. Cela montre l'importance de la coopération et de l'anticipation. Vincent Strubel (ANSSI) a souligné que la « force du collectif » a été déterminante, avec une mobilisation sans faille de tous les acteurs et un blocage des attaques très en amont, parfois même « trop tôt pour savoir quelles étaient les intentions des adversaires » . ((ANSSI), 2024)

Autrement dit, l'approche proactive adoptée (neutraliser les menaces dès les premiers signes) s'est avérée gagnante. Cette réussite repose sur une organisation minutieuse et pourra servir de modèle. A l'avenir, la préparation de tout grand événement devrait prévoir une cellule cyber intégrée, rassemblant publics et privés, entraînée régulièrement, et autorisée à intervenir de manière préventive dès le moindre signal faible. La deuxième leçon mise en avant est la nécessité de protéger l'ensemble de l'écosystème, y compris ses éléments les plus petits ou les moins matures. Paris 2024 a réussi à étendre la protection aux PME, fédérations et autres organismes moins équipés, ce qui prouve que le passage à l'échelle est possible.

Cette approche doit être pérennisée. Pour les prochains événements, il faudra associer tous les partenaires, grands et petits, aux dispositifs de sécurité, afin d'éviter qu'un maillon faible ne compromette l'ensemble. En termes de standardisation, Paris 2024 laisse derrière lui un ensemble de bonnes pratiques et de protocoles éprouvés qui pourront être réutilisés. La documentation produite (procédures, guides techniques, plans de crise) servira de base commune pour d'autres manifestations. Il est fortement possible que les organisateurs des JO futurs ou d'événements analogues (Expositions universelles, Coupes du monde sportives) s'inspirent directement du modèle français de 2024. (ANSSI, Grands Evènements Sportifs en France, évaluation de la menace 2024, 2024)

Enfin, le retour d'expérience de Tokyo 2020 (tenu en 2021) et de Rio 2016 permet de mesurer le chemin parcouru. Tokyo avait annoncé avoir fait face à 4,4 milliards d'attaques durant ses Jeux, un chiffre colossal (800 par seconde) qui illustrait l'ampleur de la menace, même si in fine seuls quelques centaines d'incidents significatifs avaient été recensés. Rio 2016 et Londres 2012 avaient eux aussi essuyé des assauts importants, avec respectivement environ un demi-milliard et 212 millions d'attaques numériques

détectées. Surtout, PyeongChang 2018 avait subi une attaque tangible qui avait affecté le déroulement des Jeux, tandis que Tokyo 2021 a connu une fuite de données notables.

En contraste, Paris 2024 n'a connu aucune interruption due au cyber, ce qui la distingue nettement des éditions précédentes. Ce bilan exceptionnel est qualifié d'« unique » par l'ANSSI prouve qu'en appliquant rigoureusement les mesures de sécurité actuelles et en mobilisant suffisamment de ressources, il est possible de déjouer même des attaques sophistiquées. Cela offre une note d'optimisme pour l'avenir. Je vous ai présenté des méthodes de défense qui deviennent de plus en plus efficaces au fil de ces expériences, rendant la tâche des cybercriminels ou des saboteurs plus ardue à chaque nouvel événement.

Conclusion

Au cours de la rédaction de ce mémoire, j'ai pu aborder différentes notions. Les technologies évoluent sans cesse, et notamment dans les infrastructures sportives depuis les années 1990. Cela permet d'intégrer des solutions qui améliorent la performance des athlètes. J'ai pu présenter les infrastructures sportives jusque dans leur profondeur en effectuant un entretien avec le DSI du Clermont Foot, actuellement en Ligue 2. Et j'ai également pu comprendre le niveau des personnes en informatique dans le milieu sportif et associatif en effectuant des ateliers de sensibilisation avec le club de badminton Castelpontin dont je suis licencié. Ces systèmes d'information ressemblent très fortement aux systèmes d'information des entreprises mais possèdent des spécificités et des exigences différentes. Les exigences sont énormément centrées autour de la disponibilité, de la continuité des activités, bien que l'intégrité et la confidentialité restent importantes.

Les attaques sur les infrastructures sportives sont majoritairement des attaques DDoS et de social engineering. La plupart des études de cas que j'ai présentées sont liées à des erreurs humaines. Les attaques par rançongiciel, l'exfiltration de données et les attaques sur les objets connectés sont souvent la conséquence d'une attaque de social engineering. Les attaques par DDoS visent les billetteries et les diffusions de matchs, tandis que les attaques XSS, PHP injection, Local File Inclusion et SQLi visent les sites web et les applications de billetterie. J'ai pu approfondir les études de cas en remontant tout le cheminement de l'attaque jusqu'au cyberattaquant.

Après cet état de l'art de toutes les attaques qui visent les infrastructures sportives, je me suis intéressé aux différentes mesures de protection qui couvrent celles-ci. Les mesures de protection mises en place arrivent à couvrir et protéger le système d'information de toutes les attaques que j'ai présentées. J'ai pu parler de la sensibilisation des utilisateurs et effectuer des ateliers avec la trésorière et le président du club de badminton Castelpontin. Ces formations étaient axées sur la gestion des mots de passe, les différentes techniques de social engineering et la sécurisation de son poste lors d'une utilisation en public. J'ai ensuite présenté l'authentification multifacteur, qui est une mesure de sécurité de plus en plus utilisée ces dernières années. J'ai présenté la ségrégation des réseaux afin de pouvoir scinder et protéger les parties administratives, la partie IoT, la partie vidéosurveillance, la partie diffusion vidéo et la partie serveurs. J'ai expliqué les différentes méthodes de chiffrement qui sont possibles et celles qui sont utilisées dans ce milieu afin de garantir la confidentialité des données personnelles, des

données des athlètes et des données des spectateurs. Les pare-feux permettent de scinder le réseau interne et le réseau externe avec des règles de filtrage. Le filtrage réseau et des URLs intègrent désormais de l'intelligence artificielle. L'IA est le sujet phare de ces dernières années avec l'essor de ChatGPT (d'OpenAI), de Gemini (de Google), de Claude (d'Anthropic) et bien d'autres. De nombreuses cyberattaques peuvent être directement traitées par les IA.

En plus des mesures de protection, j'ai effectué une étude de cas sur l'événement qui a permis de rassembler toute la planète lors de l'été 2024, les Jeux Olympiques de Paris. Cet événement a permis de faire collaborer des organisations françaises, européennes et américaines afin d'organiser un événement mondial sans accroc. Le bilan cyber de ces jeux est un bilan inédit. Malgré une hausse des attaques informatiques, aucune n'a perturbé le bon déroulement de ces jeux. Cela confirme mon état de l'art sur la cybersécurité au sein des infrastructures sportives. Les infrastructures sportives mettent en place de plus en plus de protections et deviennent des organisations sensibles.

En abordant tous ces sujets, j'ai ainsi pu répondre à ma problématique : "Comment les infrastructures sportives peuvent-elles se protéger contre les cyberattaques, compte tenu de leur forte dépendance aux technologies numériques ?". Il est nécessaire pour les infrastructures sportives aujourd'hui de se développer en cybersécurité pour rester compétitives, ne pas entacher l'image du club ou de l'infrastructure et permettre l'organisation de grands événements sportifs comme les Jeux Olympiques de Paris.

Postface

La rédaction de ce mémoire m'a permis d'approfondir toutes les connaissances que j'ai acquises au sein de l'École Hexagone. J'ai pu approfondir ces connaissances au sein de mon entreprise en mettant en place des solutions et des mécanismes de cybersécurité. C'est notamment dans le cadre de ce mémoire que j'ai pu réaliser mes sensibilisations cybers et un audit de sécurité.

Je me sens satisfait par mon travail et mes recherches, d'autant plus que c'est un sujet qui n'a jamais été abordé, allier sport et cybersécurité. J'ai pu facilement trouver une première version de ma problématique en cherchant dans mon domaine de compétence ainsi que dans ma passion. Je porte un fort intérêt pour le domaine de la cybersécurité, c'est un domaine large qui, même s'il ne faisait pas partie de mes études au départ, m'a permis de découvrir de nombreux domaines de compétences. L'évolution des technologies est de plus en plus rapide, et cela devient difficile à suivre. Je voulais donc à travers mon mémoire faire un tour d'horizon sur les principales attaques au sein des infrastructures sportives ainsi que les protections qui sont associées.

J'ai aimé ce travail de recherches, contacter et effectuer des entretiens avec des Directeurs des Systèmes d'Informations et des Responsables Sécurité des Systèmes d'information. Cela m'a permis d'en apprendre plus sur le sujet et d'étendre mon réseau professionnel.

Bibliographie

(ANSSI), V. S. (2024). *Vincent Strubel (ANSSI) : « Un bon niveau d'inquiétude » en termes de cybersécurité*. Récupéré sur https://www.lequipe.fr/Tous-sports/Actualites/Vincent-strubel-anssi-un-bon-niveau-d-inquietude-en-termes-de-cybersecurite/1407650

Adam, S. (2024). *The State of Ransomware 2024*. Récupéré sur Sophos: https://news.sophos.com/en-us/2024/04/30/the-state-of-ransomware-2024/

AFP. (s.d.). *"Football Leaks": Rui Pinto reconnaît avoir recouru au piratage informatique*. Récupéré sur https://www.la-croix.com/Lanceur-alerte-pirate-informatique-source-Football-Leaks-barre-2022-10-10-1301236926

Akamai. (2024). *State of the Internet Reports*. Récupéré sur https://www.akamai.com/security-research/the-state-of-the-internet

ANSSI. (2020). *Attaques par rançongiciels, tous concernés*. Récupéré sur https://cyber.gouv.fr/publications/attaques-par-rancongiciels-tous-concernes

ANSSI. (2023). *Panorama de la cybermenace 2023*. Récupéré sur https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

ANSSI. (2024). *Grands Evènements Sportifs en France, évaluation de la menace 2024*. Récupéré sur https://cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-003.pdf

ANSSI. (s.d.). *La cybersécurité des systèmes industriels*. Récupéré sur La cybersécurité des systèmes industriels: https://cyber.gouv.fr/publications/la-cybersecurite-des-systemes-industriels

ANSSI. (s.d.). *NP_Guide_DDoS*. Récupéré sur https://cyber.gouv.fr/sites/default/files/2015/03/NP_Guide_DDoS.pdf

BARRAT, C. t. (2024). *Sabotage informatique des JO : l'exemple d'Olympic Destroyer à Pyeongchang en 2018*. Récupéré sur https://citalid.com/fr/resources/sabotage-informatique-jo-olympic-destroyer/

BURNEL, F. (2022). *Qu'est-ce qu'une attaque DDoS*. Récupéré sur IT Connect FR: https://www.it-connect.fr/quest-ce-quune-attaque-ddos/

CNIL. (2024). *Guide de la sécurité des données personelles* . Récupéré sur https://www.cnil.fr/sites/cnil/files/2024-03/cnil_guide_securite_personnelle_2024.pdf

CNIL. (s.d.). *CHAPITRE II - Principes*. Récupéré sur CHAPITRE II - Principes: https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2

Cohen, D. (s.d.). *VLAN : Qu'est-ce qu'un réseau LAN virtuel, et quel est son rôle ?* Récupéré sur DataScientest: https://datascientest.com/vlan-tout-savoir

CTI-TEAM. (2024). *Sabotage informatique des JO : l'exemple d'Olympic Destroyer à Pyeongchang en 2018*. Récupéré sur Sabotage informatique des JO : l'exemple d'Olympic Destroyer à Pyeongchang en 2018: https://citalid.com/fr/resources/sabotage-informatique-jo-olympic-destroyer/

CyberArk. (2023). *Privileged Access Management*. Récupéré sur CyberArk: https://www.cyberark.com/fr/what-is/privileged-access-management/

Cyberdéfense, O. (2024). *Jeu, Set et Hack : quand les cybercriminels s'attaquent aux billetteries des événements sportifs*. Récupéré sur https://www.orangecyberdefense.com/ar-ma/insights/blog/cybercriminels-billetterie-sport?utm_source=linkedin&utm_medium=social&utm_campaign=resources

Diaries, D. (2020). *EP 64 : The Athens Shadow Games*. Récupéré sur https://darknetdiaries.com/transcript/64/

Diaries, D. (2020). *EP 77 : Olympic Destroyer*. Récupéré sur https://darknetdiaries.com/episode/77/

DILKOFF, D. (2024). *Paris 2024 : le détail d'un dispositif de sécurité hors normes*. Récupéré sur https://www.lemonde.fr/societe/article/2024/07/22/paris-2024-le-detail-d-un-dispositif-de-securite-hors-normes_6255160_3224.html

Finkle, A. B. (2016). *Anti-doping agency says athlete data stolen by Russian group*. Récupéré sur https://www.reuters.com/article/us-doping-wada-cyber/anti-doping-agency-says-athlete-data-stolen-by-russian-group-idUSKCN11J26T/

Fortinet. (s.d.). *Qu'est-ce que la triade CIA ?* Récupéré sur Qu'est-ce que la triade CIA ?: https://www.fortinet.com/fr/resources/cyberglossary/cia-triad

GANGLOFF, Y. (2020). *En Angleterre, une loi pour sécuriser l'IoT va être présentée*. Récupéré sur https://siecledigital.fr/2020/01/31/en-angleterre-une-loi-pour-securiser-liot-va-etre-presentee/

Gatewatcher. (s.d.). *L'épreuve non-sportive des Jeux Olympiques et Paralympiques de Paris : la course à la cybersécurité*. Récupéré sur https://www.gatewatcher.com/lab/lepreuve-non-sportive-des-jeux-olympiques-et-paralympiques-de-paris-la-course-a-la-cybersecurite/

Gouv, D. (s.d.). *Entrainement Drones Tactiques pour JO 2024*. Récupéré sur Entrainement Drones Tactiques pour JO 2024: https://www.defense.gouv.fr/operations/actualites/entrainement-drones-tactiques-zone-urbaine-cadre-jeux-olympiques-paralympiques-paris-2024

HARRINGTON, D. (2023). *Sécurité des données : importance, types et solutions*. Récupéré sur https://www.varonis.com/fr/blog/securite-donnees

IBM. (2024). *Qu'est-ce que le BYOD (bring your own device) ?* Récupéré sur IBM: https://www.ibm.com/fr-fr/topics/byod

iTech, L. S. (2024). *Stades connectés - Quelles technologies*. Récupéré sur https://www.lesport-itech.com/2024/01/02/stades-connectes-quelles-technologies/

Légifrance. (s.d.). *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. Récupéré sur Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés: https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037822959

Les Jeux Olympiques 2024 : Un grand événement sportif où des enjeux sûreté, cybersécurité et réputations se superposent. (2021). Récupéré sur

https://www.ege.fr/sites/ege.fr/files/media_files/S%C3%A9curisationJO2024.pdf

MARCOU, P.-P. (2024). *Le groupe d'informatique Atos doit faire le deuil des Jeux olympiques*. Récupéré sur https://www.lemonde.fr/economie/article/2024/08/10/le-groupe-d-informatique-atos-doit-faire-le-deuil-des-jeux-olympiques_6275101_3234.html

Matlink. (2015). *Le chiffrement homomorphe*. Récupéré sur https://blog.matlink.fr/chiffrement-homomorphique-2/

Ministère des sports, d. l. (s.d.). *Principaux textes de référence pour les équipements sportifs*. Récupéré sur https://www.sports.gouv.fr/principaux-textes-de-reference-pour-les-equipements-sportifs-842

Monmarché, K. (2023). *Stormshield integrates Bitdefender URL filtering and continues to consolidate its European trust offering*. Récupéré sur Stormshield: https://www.stormshield.com/news/stormshield-integrates-bitdefender-url-filtering-and-continues-to-consolidate-its-european-trust-offering/

Neskey, C. (s.d.). *Are Your Passwords in the Green?* Récupéré sur Hive Systems: https://www.hivesystems.com/blog/are-your-passwords-in-the-green

PAULS, G. (2023). *Sport, La cybersécurité s'invite sur le terrain*. Récupéré sur https://www.orangecyberdefense.com/fr/insights/blog/sport-la-cybersecurite-sinvite-sur-le-terrain

Proofpoint. (s.d.). *Qu'est-ce que le typosquatting ?* Récupéré sur Qu'est-ce que le typosquatting ?: https://www.proofpoint.com/fr/threat-reference/typosquatting

Radware. (2024). *Les 7 types d'attaque les plus fréquents que le pare-feu d'applications web (WAF) est conçu pour arrêter*. Récupéré sur Radware: https://fr.radware.com/cyberpedia/application-security/7-most-common-attack-types/

RGPD, E. (s.d.). *"Traitement portant sur des catégories particulières de données à caractère personnel"*. Récupéré sur "Traitement portant sur des catégories

particulières de données à caractère personnel": https://www.privacy-regulation.eu/fr/9.htm

School, C. M. (s.d.). *Données sensibles RGPD : comment sont collectées et traitées vos informations privées ?* Récupéré sur https://www.cyber-management-school.com/ecole/les-fondamentaux-de-la-cybersecurite/donnees-sensibles-traitement-collecte/

SIEGEL, B. (2019). *Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread*. Récupéré sur Security Boulevard: https://securityboulevard.com/2019/07/ransomware-amounts-rise-3x-in-q2-as-ryuk-sodinokibi-spread/

Swain, G. (2024). *Chinese researchers break RSA encryption with a quantum computer*. Récupéré sur CSO: https://www.csoonline.com/article/3562701/chinese-researchers-break-rsa-encryption-with-a-quantum-computer.html

Trevino, A. (2024). *What Is Shoulder Surfing?* Récupéré sur Keeper: https://www.keepersecurity.com/blog/2023/07/26/what-is-shoulder-surfing/

Wikipédia. (2025). *Ingénierie sociale*. Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/Ing%C3%A9nierie_sociale_(s%C3%A9curit%C3%A9_de_l%27information)