CYBERSECURITE ET INFRASTRUCTURES RESEAUX DANS LE SECTEUR SPORTIF

Réseau / Cybersécurité

Résumé Les infrastructures sportives modernes, comme les stades ou les complexes multisports, nécessitent des réseaux robustes et sécurisés pour gérer divers besoins :

Wi-Fi pour les spectateurs, systèmes de paiement, caméras de surveillance, diffusion en direct et outils de gestion interne.

Valentin Broennec
BTS SIO 1

Sommaire

Introduction

Cybersécurité et infrastructure réseau

L'industrie du sport est aussi sensible aux cyberattaques que n'importe quelle autre grande entreprise. Actuellement, les attaques contre les grands événements sportifs se multiplient. En général, ces attaques consistent à bloquer l'accès aux services de streaming avec des revendications particulières.

L'infrastructure numérique évolue sans cesse, et les responsables de la sécurisation doivent constamment se mettre à jour pour assurer le maintien du réseau en continu. Les coûts financiers de ces attaques sont stupéfiants, le piratage représentant des pertes de plusieurs milliards de dollars pour l'industrie du sport chaque année.

Je développerai ce sujet en plusieurs parties. Dans la première, j'expliquerai les moyens employés pour construire et développer un système réseau efficace et protégé contre toute attaque. Dans

la deuxième, je détaillerai les méthodes mises en place par les techniciens pour sécuriser les diffusions sportives via les plateformes de streaming et à la télévision. Ensuite, j'analyserai les raisons de ces attaques ainsi que leurs impacts financiers et humains. Enfin, je conclurai en abordant les évolutions futures du réseau et de la cybersécurité dans le domaine du sport.

La stratégie de sécurisation des évènements sportif

Les complexes sportifs modernes (stades, salles de sport, circuits automobiles, etc.) nécessitent une infrastructure réseau robuste pour répondre à plusieurs besoins simultanés telle que la connexions Wi-Fi pour des milliers de spectateurs, Transmission des flux vidéo en direct pour la diffusion TV et streaming, gestion des systèmes de billetterie et des paiements électroniques, sécurité avec vidéosurveillance et contrôle d'accès, communication interne entre le personnel et les joueurs.

Tous ces éléments doivent être pris en compte pour réfléchir à un plan d'action, une architecture réseau bien conçue est indispensable. Elle repose sur une segmentation intelligente, des équipements performants et des protocoles de sécurisation adaptés. Un complexe sportif utilise généralement une topologie en étoile ou maillée, selon les besoins en redondance et en performance.

Le réseau en étoile

Le réseau en étoile est utilisé lorsque le stade ou le lieu de l'événement sportif dispose d'un datacenter centralisé qui distribue la connexion à tous les équipements via des switchs et des routeurs. Cela présente l'avantage d'une gestion simplifiée et d'une centralisation des données, ce qui facilite les sauvegardes et la gestion de l'information. De plus, cette architecture permet de détecter plus facilement une tentative d'attaque.

Cependant, son principal inconvénient est qu'elle repose sur un seul et unique serveur et switch. En cas de panne de l'un d'eux, l'ensemble du réseau devient inopérant, ce qui représente un risque majeur pour la continuité du service.

Le réseau maillé

Cette méthode est employée pour les plus grands événements, comme la Coupe du Monde ou la Formule 1, qui ont l'habitude de gérer une forte densité de connexions simultanées.

L'objectif de cette infrastructure est que chaque nœud (switch, routeur, point d'accès Wi-Fi) soit relié à plusieurs autres, offrant ainsi plusieurs chemins pour les données. Cela permet une meilleure tolérance aux pannes, car si un équipement tombe en panne, un autre peut automatiquement prendre le relais. Cette redondance assure une plus grande fiabilité par rapport à la méthode précédente.

Cependant, cette solution est bien plus coûteuse, et sa configuration est plus complexe. Elle nécessite également un personnel qualifié pour la mise en place et la gestion du réseau

Segmentation du réseau avec VLAN

Évidemment, la segmentation du réseau est nécessaire, non seulement pour la sécurité qu'elle apporte, mais aussi pour la gestion des flux en fonction de l'utilisation. Dans un stade, au lieu que tous les équipements soient sur un seul réseau, on peut créer des VLAN distincts, comme :

VLAN 10 : Administratif (PC du personnel, serveurs internes)

VLAN 20 : Wi-Fi public (Smartphones et tablettes des spectateurs)

VLAN 30 : Diffusion vidéo (Caméras, serveurs de streaming)

VLAN 40 : Sécurité (Caméras de surveillance, contrôle d'accès)

VLAN 50 : Médias et presse (Postes des journalistes)

Un réseau unique avec tous les équipements mélangés génère beaucoup de trafic, ce qui peut provoquer des ralentissements. Avec des VLAN, le trafic est isolé et mieux réparti, réduisant ainsi la congestion. De plus, certains équipements ne doivent pas pouvoir communiquer entre eux. Par exemple, le Wi-Fi public ne doit pas pouvoir accéder aux serveurs administratifs. De même, le VLAN des caméras de surveillance doit être isolé pour éviter qu'un pirate ne prenne le contrôle du système.

Ce qui est pratique avec l'utilisation de la segmentation du réseau, c'est aussi la priorisation du trafic, ce qu'on appelle QoS. Cela permet de donner plus de bande passante au streaming vidéo qu'au Wi-Fi public. De manière plus générale, la segmentation avec VLAN est une solution essentielle pour organiser un réseau efficacement, en séparant les flux de données, en renforçant la sécurité et en améliorant les performances. Dans un environnement comme un complexe sportif, cela permet d'assurer un service fiable pour tous les utilisateurs, tout en protégeant les données sensibles et en réduisant la congestion du réseau.

L'équipement nécessaire

Un réseau performant dans un complexe sportif repose sur plusieurs équipements essentiels. Les équipements présentés ci-dessous sont tous plus ou moins utilisés dans le monde du sport et de son infrastructure. Il est évident que ce matériel a un coût qui peut atteindre des millions d'euros lors des plus grands événements, mais il est nécessaire pour assurer le bon fonctionnement des services proposés.

Switchs et routeurs : Le cœur du réseau

Les switchs et routeurs sont indispensables pour assurer la circulation des données à l'intérieur du complexe sportif et vers l'extérieur. Il existe deux niveaux de switchs dans le monde professionnel. Le premier est le niveau 2, avec des modèles comme les switchs Cisco Catalyst 2960 ou HP Aruba 2530. Ceux-ci permettent de gérer les connexions entre appareils au sein d'un même VLAN et fonctionnent principalement avec les adresses MAC. Il existe aussi des switchs de niveau 3, comme le Cisco Catalyst 3850 ou le Juniper EX4300, qui sont capables de gérer le routage inter-VLAN et d'appliquer des règles de sécurité avancées. Dans un stade, les switchs sont généralement placés dans des armoires techniques réparties dans tout le complexe pour assurer une couverture uniforme.

Les routeurs, quant à eux, connectent le réseau interne du stade à Internet et assurent la gestion des flux de données vers les plateformes de streaming, les médias et les services administratifs. Parmi les modèles les plus connus, on trouve les Cisco ISR 4000 Series et le Juniper MX Series. Ces équipements permettent de gérer les connexions Internet et VPN, d'assurer le routage des paquets entre VLAN et vers l'extérieur, et d'appliquer les règles de QoS pour prioriser certains types de trafic.

Infrastructure Wi-Fi : Connexion pour le public et le staff

Un complexe sportif accueille des milliers de spectateurs, chacun utilisant son smartphone ou sa tablette pour naviguer sur Internet, regarder des replays ou interagir sur les réseaux sociaux. Certes, on pourrait penser que tout le monde utilise désormais la 4G/5G, mais chaque lieu sportif dispose tout de même de son Wi-Fi public, qui, malgré la connexion mobile, reste toujours nécessaire. Ainsi, une infrastructure Wi-Fi robuste est cruciale.

Les points d'accès Wi-Fi (AP - Access Points) distribuent le signal sans fil aux spectateurs et au personnel. Dans un grand stade, plusieurs centaines de points d'accès sont installés pour couvrir l'ensemble des gradins, les couloirs, les loges VIP et les zones techniques. Il existe le WiFi 6 et le Wi-Fi 6E, qui sont de plus en plus déployés partout et donc deviennent de plus en plus accessibles. Ces technologies permettent une connexion rapide et stable avec moins d'interférences, couplées au MIMO (Multiple Input, Multiple Output), qui permet à plusieurs appareils de se connecter simultanément sans perte de performance. Ces deux technologies sont nécessaires pour le maintien du réseau Wi-Fi public. Dans un stade, les points d'accès sont souvent placés sous les sièges, au plafond ou sur des pylônes pour maximiser la couverture et éviter les obstacles physiques.

Serveurs et stockage

Les événements sportifs sont souvent diffusés en direct, que ce soit sur des plateformes de streaming ou à la télévision. Par exemple, le sport que je pratique, le badminton, possède sa propre chaîne dédiée, tandis que les plateformes de streaming varient. Ces flux vidéo doivent être encodés, stockés temporairement et envoyés à des serveurs distants.

Les catégories de serveurs utilisés sont les serveurs IPTV, qui convertissent les flux vidéo en un format compatible avec les plateformes de streaming. Les serveurs CDN (Content Delivery Network) répartissent le trafic vidéo entre plusieurs centres de données pour éviter les ralentissements. Enfin, les serveurs de replays et de VOD stockent les vidéos pour permettre aux spectateurs de revoir les moments forts.

Ces serveurs ne sont pas forcément sur place, sauf pour les serveurs de diffusion en direct, qui eux, sont souvent situés sur site. En revanche, les données peuvent être externalisées vers des data centers qui centralisent tous les replays ou autres types de rediffusion. Les stades modernes utilisent des serveurs sur site couplés à des solutions cloud (AWS, Azure) pour assurer une diffusion fluide et rapide.

Sécurité et supervision du réseau

Un réseau de stade est une cible privilégiée des cyberattaques (DDoS, intrusions, phishing). Des équipements spécifiques sont mis en place pour garantir une sécurité optimale comme le firewall analyse le trafic réseau pour bloquer les connexions suspectes. Un IDS/IPS (Intrusion Detection & Prevention System) détecte et empêche les attaques en temps réel. Evidemment les plus connu sont utilisé : Fortinet FortiGate, Palo Alto Networks, Cisco ASA.

Les acteurs de cette organisation

Organisation et planification en amont d'un événement

Dans un complexe sportif de grande envergure, la gestion du réseau et de la cybersécurité est assurée par plusieurs équipes spécialisées. Bien entendu, lors d'événements mondiaux tels que la Coupe du Monde de Rugby ou les Jeux Olympiques, les enceintes sportives sélectionnées sont régies par la réglementation des autorités nationales et des fédérations sportives. Trois principaux acteurs ont la charge de leur application : l'organisateur de l'événement, la préfecture et la ville hôte.

Sauf exception, les collectivités hôtes sont responsables des infrastructures sportives mises à disposition pour l'évènement et de la sécurisation des Systèmes d'Information associés. Ainsi, en amont de ces évènements, différentes actions sont préconisées par les autorités (réalisation d'une analyse de risques, sensibilisation des collaborateurs, réalisation d'un Plan de Continuité/Reprise d'Activité, etc.) dans le but d'effectuer un état des lieux de l'existant et d'en déduire les chantiers à réaliser. Cette étape est essentielle pour augmenter le niveau de sécurité et de maturité cyber des infrastructures.

Il y a aussi L'ANSSI qui est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Elle propose au Premier ministre les mesures destinées à répondre aux crises affectant ou menaçant l'intégrité numérique de la Nation et coordonne l'action gouvernementale en matière de défense des systèmes d'information. Elle anime, coordonne les travaux interministériels en matière de sécurité du numérique et élabore les mesures de protection des systèmes d'information, en veillant à l'application de celles-ci notamment par le biais d'audits. Depuis juillet 2022, le pilotage de la stratégie de prévention des cyberattaques en vue des Jeux Olympique de Paris est confié à l'Agence nationale de la sécurité des systèmes d'information.

Le risque zéro en matière de cybersécurité n'existe pas. L'évolution du marché de la sécurité tend vers le zéro trust (zéro confiance par défaut). Il s'agira en priorité d'être vigilant à la fois sur le contrôle d'accès aux réseaux informatiques, sur la protection des utilisateurs, des postes de travail, des données et des applications. Voice les étapes globales d'une bonne préparation à un évènement sportif :

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

Les conséquences d'une cyber attaque

Tous les plus grands événements, de la Coupe du monde de football au Super Bowl, en passant par le cyclisme et le tennis, tous représentent des cibles lucratives pour les cyberattaques en raison de leur envergure mondiale, de leur impact économique et de leur dépendance aux technologies numériques pour différents aspects opérationnels.

Les cyberattaquants sont susceptibles de cibler les systèmes numériques de ces événements (c'est-à-dire les systèmes de billetterie et de notation) et les plateformes de gestion d'événements, les canaux d'engagement des fans, ainsi que les services de streaming en ligne et les réseaux de diffusion pour perturber les opérations ou voler des informations sensibles.

Une grande visibilité à travers le monde

Avec des millions de spectateurs, d'athlètes, de sponsors et une couverture médiatique du monde entier, toute perturbation ou compromission pendant l'événement peut attirer une attention significative, permettant aux acteurs menaçants d'acquérir une notoriété et de nombreuses opportunités de faire avancer leurs programmes. En tenant compte de la vente de billets, des droits de diffusion, des parrainages, des marchandises et des revenus touristiques, les évènements sportifs représentent une industrie de plusieurs milliards de dollars offrant de nombreuses opportunités aux acteurs malveillants de rechercher un gain financier (par exemple : fraude aux billets, marchandises contrefaites, attaques de ransomwares), ou vol d'informations financières sensibles auprès d'athlètes, de sponsors ou de participants).

Des perturbations politiques et idéologiques.

Ces compétitions constituent une cible potentielle pour les acteurs malveillants ayant des motivations politiques ou idéologiques. Les acteurs étatiques, les groupes hacktivistes ou les organisations extrémistes peuvent chercher à perturber ou à saper l'événement pour faire avancer leurs programmes politiques, provoquer des tensions géopolitiques ou promouvoir leurs causes. Suite à la suspension de la Russie pour dopage d'État et à l'interdiction de World Athletics suite à l'invasion de l'Ukraine, l'événement a fait l'objet de lourdes attaques de la part d'acteurs menaçants russes cherchant à faire valoir des arguments politiques.

L'impact de la cybersécurité dans le sport est déjà visible. Par exemple, en 2020, l'équipe de Formule 1 de Williams Racing a été victime d'une cyberattaque lors d'un événement virtuel. De même, plusieurs clubs de football ont été ciblés par des ransomwares, mettant en péril leurs données sensibles.

Un exemple récent et frappant de la menace croissante que représentent les cyberattaques pour le monde du sport est l'attaque contre la Fédération française de rugby (FFR). Selon des informations confirmées, la FFR a été ciblée par le groupe de pirates informatiques Play. Cette attaque a principalement affecté les serveurs de messagerie de la FFR. Les cybercriminels ont menacé de dévoiler des informations confidentielles, notamment des données personnelles d'employés et des passeports, si la FFR ne négociait pas avec eux

Conclusion

Souvent, les technologies de sécurité ont la réputation d'être complexes et de ralentir les systèmes. Par conséquent, de nombreuses entreprises renoncent à la sécurité de réseau au profit de la performance. La cybersécurité doit être capable de suivre et ne pas ralentir ce processus. Cela signifie qu'elle doit fournir à la fois une sécurité et une performance maximales.

Annexes

Sources

- https://www.orangecyberdefense.com/fr/insights/blog/sport-la-cybersecurite-sinvitesur-le-terrain
- https://www.forbes.fr/technologie/cybersecurite-et-sport-proteger-lepine-dorsalenumerique-des-evenements-sportifs/
- https://www.cyber-management-school.com/actualite/la-cybersecurite-dans-le-sport/
- https://patrickbayeux.com/actualites/evenements-sportifs-et-cyberattaques-quelsenjeux/
- https://www.informatiquenews.fr/les-enceintes-sportives-doivent-controler-leursfournisseurs-pour-garantir-la-cybersecurite-ashish-khanna-verizon-100094
- https://fr.linkedin.com/pulse/limpact-de-la-cybersécurité-dans-le-sport-karlismontchovi
- https://cyber.gouv.fr/actualites/lanssi-et-le-bsi-publient-un-rapport-sur-lacybersecurite-des-grands-evenements-sportifs
- https://incyber.org/article/cybersecurite-et-formule-1-un-exemple-a-suivre/
- https://www.cisco.com/c/fr_ca/support/docs/switches/catalyst-6000-seriesswitches/10589-75.html?utm_source=chatgpt.com
- https://www.biotime-technology.com/limportance-des-protocoles-ouverts-pour-lasecurite-dans-les-infrastructures-sportives/?utm_source=chatgpt.com*
- https://www.corning.com/data-center/emea/fr/home/knowledge-center/cabling-thespine-and-leaf-network-switch-fabric.html?utm_source=chatgpt.com