https://www.nouvelobs.com/economie/20200128.OBS24047/et-si-des-hackeurs-pirataient-le-stade-de-france-pendant-les-jo-2024.html

Et si des hackeurs pirataient le Stade de France pendant les JO 2024 ?

Foule des spectateurs en liesse lors de la finale de l'Euro de football au Stade de France (VALERY HACHE / AFP)

Entièrement informatisés, les stades font désormais partie des structures sensibles à protéger des pirates, en particulier à l'approche des jeux Olympiques.

Par Thierry Noisette (Thierry Noisette, à Vannes (Morbihan))

Publié le 28 janvier 2020 à 15h05

Stade de France, le 1er août 2024 : 70 000 spectateurs se sont massés pour acclamer les athlètes olympiques qui s'apprêtent à s'élancer sur la piste. Soudain, sirènes et lampes clignotantes se déclenchent partout dans l'enceinte. Un message « Evacuation immédiate, danger ! » remplace les publicités vidéo des abords du stade. La foule tente de fuir dans tous les sens, mais une partie des issues est verrouillée. Dans la panique, de nombreux spectateurs sont piétinés… Tout ça à cause d'une attaque informatique.

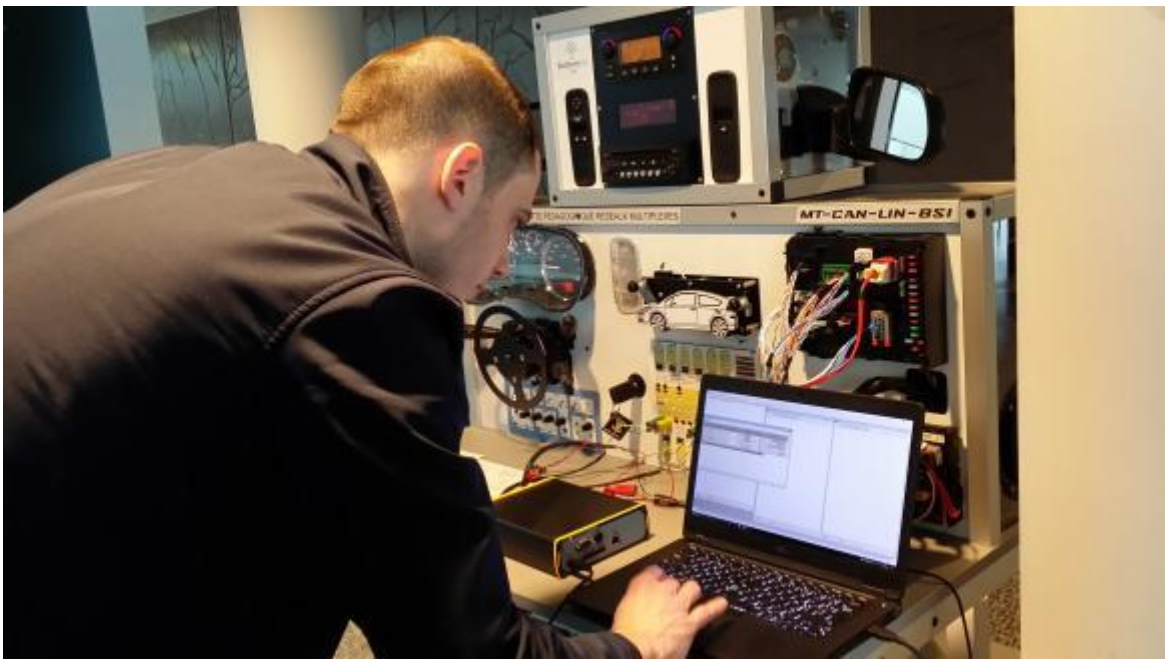
Ce scénario catastrophe est loin d'être fantaisiste. *« Plus on numérise, plus on augmente la surface d'attaque »*, confirme Salah Sadou, responsable scientifique à l'Ecole nationale supérieure d'Ingénieurs de Bretagne Sud (Ensibs) de l'université Bretagne-Sud (UBS).
En 2007, le site web du stade accueillant la finale du championnat de football américain Super Bowl a été piraté. En 2024, c'est le stade lui-même qui pourrait être victime de piratage. Aussi

bien à l'occasion d'un événement sportif, comme les jeux Olympiques, que lors d'un grand concert ou spectacle, réveillant le spectre des attentats du 13-Novembre.

C'est en tout cas le genre d'hypothèses sur lesquelles planche l'UBS. Thomas Toublanc, ingénieur d'études, prévient :

« Allumer ou éteindre les projecteurs, ouvrir ou fermer des barrières, déclencher des alarmes, des lumières d'incendie, afficher de la propagande ou des fausses alertes sur les panneaux publicitaires… de nombreux usages malveillants sont possibles. »

Et il n'y a pas que les failles technologiques que l'équipe technique doit parer, toute l'organisation doit être revue en détail – ce que les spécialistes appellent « systèmes de systèmes sociotechniques » (SdSST).



A l'école d'ingénieurs de l'université Bretagne Sud, les étudiants en cybersécurité utilisent cette reconstitution des systèmes numériques d'une voiture pour en comprendre les failles. (THIERRY NOISETTE POUR L'OBS)

Anticiper les « trous dans la raquette »

Voici un des scénarios donnés à l'UBS : dans un stade, des équipements informatiques supplémentaires ont été ajoutés dans un local, à l'occasion d'un événement. Ils chauffent trop et un capteur de température déclenche une alarme, ce qui fait venir un technicien. Il laisse ouverte une porte pour refroidir la pièce, mais une autre urgence l'appelle et il s'en va sans la refermer. Plus aucun mot de passe, badge ou autre barrière ne protège alors le local. Pas besoin de compétences pointues en hacking, un simple curieux pourrait aisément pénétrer dans l'enceinte et faire des dégâts, volontaires ou non. Ce genre de « trou dans la raquette » doit aussi être anticipé par l'équipe technique, qui imagine toutes sortes de déroulements et de protocoles. Selon Thomas Toublanc :

« Un exemple de solution pour ce scénario est un verrouillage de l'organe de commande, avec de la reconnaissance faciale au lieu du mot de passe, car le port de gants pourrait gêner les techniciens pour la saisie du code. »

Les pirates misent souvent, voire plus, sur le comportement humain que sur la technologie. Chez Veyan, société morbihannaise de conseil en sécurisation du patrimoine numérique, on cite un test effectué : l'envoi par mail aux salariés d'une entreprise d'un prétendu CV de neveu, émanant en apparence d'une personne de confiance. Quarante des destinataires ont cliqué sur la pièce jointe, un PDF truqué. S'il venait de vrais pirates, ce fichier aurait ouvert la porte à une intrusion.

A l'UBS-Ensibs, une maquette polyvalente sur laquelle les étudiants, grâce à des simulations, apprennent à déjouer les vulnérabilités. (THIERRY NOISETTE POUR L'OBS)

Mi-mars, l'UBS créera une nouvelle chaire « Cybersécurité des grands événements publics ». Pour Salah Sadou, son directeur scientifique, *« tous les problèmes de cybersécurité sont transdisciplinaires »* et il s'agira *« que nos recherches servent à la prévention des attaques contre les Jeux : un événement comme les JO, c'est un système de systèmes sociotechniques, dans lequel il y a du hard, du soft, de l'organisation etc. »*

Pour préparer cette chaire, ses responsables dans l'université vannetaise ont rencontré la Coordination nationale pour la sécurité des jeux Olympiques 2024 et la gendarmerie nationale. *« Outre la cybersécurité des stades,* précise Anne Le Hénanff, cotitulaire de la chaire, *les thésards et leurs enseignants s'intéresseront à tout l'écosystème des grands événements sportifs : les transports, les médias, l'hébergement et les équipements des sportifs, les réseaux électriques, téléphoniques… »*

Au-delà des JO et du sport, tous les aspects de la cyberdéfense font de la discipline un secteur d'avenir : les effectifs cyber de l'UBS devraient presque doubler d'ici trois à quatre ans, passant de 350 à 600 étudiants. *« Il n'y a pas de problème de chômage dans ces filières-là »*, souligne Jack Noël, coordinateur du Centre de cybersécurité de l'UBS.