DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

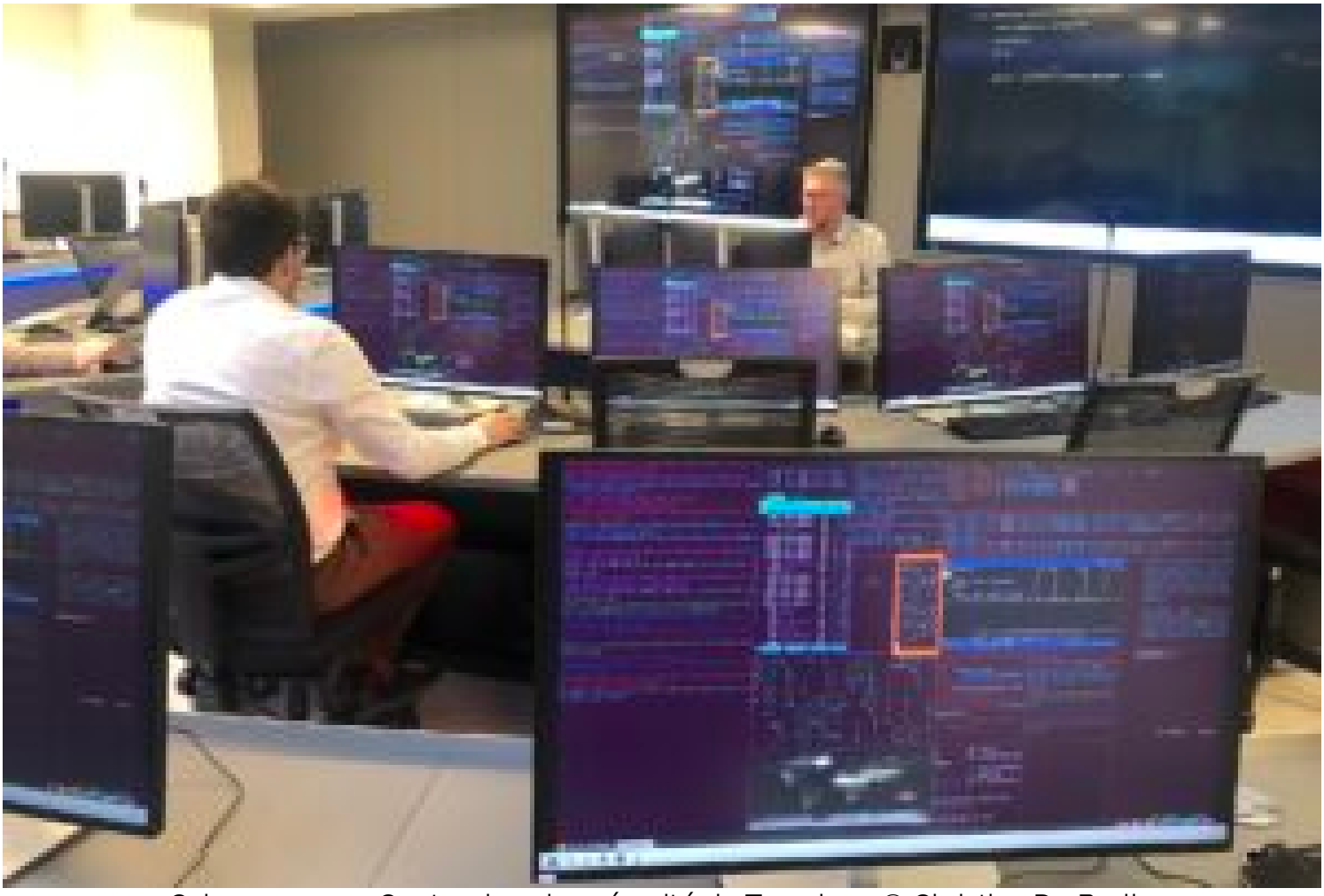
A TRANSINNE, LE CENTRE DE CYBERSÉCURITÉ SE DRESSE CONTRE LES PIRATES INFORMATIQUES

Publié le 4 mars 2025

Les activités d'un hôpital se retrouvent soudainement bloquées suite au piratage de son système informatique. Voilà un scénario qui ne relève malheureusement plus de la science-fiction. Pour prévenir ce genre de problème, un tout nouveau centre wallon consacré à la cybersécurité vient de voir le jour à Transinne : le « Centre Cybersécurité Idelux ». Et il ne s'adresse pas qu'aux institutions hospitalières désireuses de mieux se protéger!

« Notre Centre combine sur un seul site deux infrastructures uniques en Europe », explique Pierre-Yves Defosse, business developper chez Idelux. « Il dispose d'un laboratoire de cryptographie quantique et d'un cyber range, soit un outil qui permet aux institutions publiques et semi-publiques, mais aussi aux entreprises, d'apprendre à mieux lutter contre la cybercriminalité. Notre Centre est accessible à tous les acteurs économiques, publics, industriels et académiques concernés par la cybersécurité dans notre Région et ce, gratuitement.»

DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"



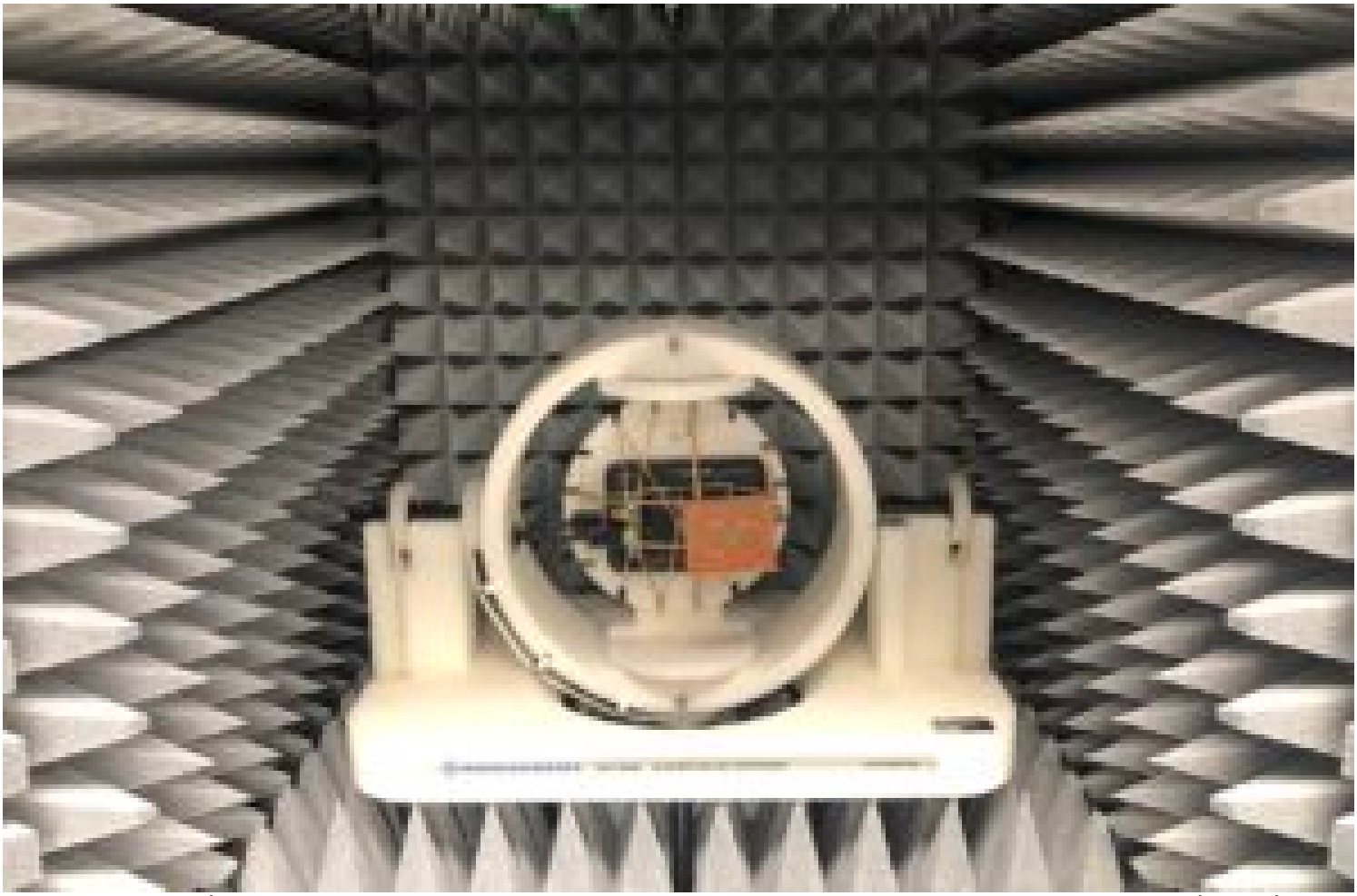
Cyber range au Centre de cybersécurité de Transinne © Christian Du Brulle

Un labo de cryptographie quantique au service des chercheurs

La gestion du laboratoire de cryptographie quantique a été confiée au groupe Thales. Il s'adresse aux chercheurs, aux ingénieurs et autres spécialistes qui travaillent sur de nouvelles technologies basées sur la physique quantique. Et ce, afin de mieux sécuriser les communications numériques. La cryptographie quantique, notamment la distribution quantique de clés (QKD), offre un niveau de sécurité inégalé en rendant toute tentative d'interception détectable.

« Ce laboratoire est un outil didactique et de recherche. Il dispose de différents équipements, comme une chambre anéchoïque ou encore d'un système de cryptage qu'on ne retrouve pas souvent dans les universités », précise Jonathan Pisane (Thales). « Cela permet, notamment, de tester des algorithmes de chiffrement, de vérifier si ce chiffrement est compatible avec la latence, d'émuler (simuler sur ordinateur, NDLR) des situations réelles, de tester des scénarios réalistes. »

La chambre, dite « anéchoïque », du laboratoire se présente sous la forme d'une petite armoire dont les parois internes sont munies d'un ensemble de blocs de mousse qui absorbent les ondes électromagnétiques, évitant ainsi des effets d'écho. C'est l'idéal pour travailler sur des antennes innovantes utilisant diverses fréquences.



Chambre anéchoïque au laboratoire de cryptographie quantique du Centre de Cybersécurité de Transinne © Christian Du Brulle

Simulateur de cyberattaques

Les institutions et les entreprises doivent désormais se prémunir au mieux contre le piratage informatique. Une directive européenne, baptisée NIS2, et qui va dans ce sens, a été transposée dans le droit belge l'an dernier.

Le « cyber range » du nouveau Centre de cybersécurité de Transinne et son simulateur de crise sont donc le lieu idéal pour s'entraîner. « Nos équipements permettent aux équipes professionnelles de se former de manière concrète et performante à la cybersécurité », explique Johan Helin, de la société Nexova Cyber, spécialisée en cybersécurité et chargée de ces formations. « À partir de scénarios réalistes d'attaques et de ripostes, les utilisateurs peuvent tester la résilience de leur système et anticiper les cybermenaces. »

« Notre but est de les amener à détecter et à répondre correctement à une menace, que nous provoquons volontairement dans la simulation », précise M. Helin. « Cela sert aussi à tester des procédures existantes. On peut recréer des situations dans n'importe quel domaine : maritime, ferroviaire, énergétique, bancaire, dans une PME, une usine, une chaîne de fabrication… Notons aussi que cela peut également être utile à la maison, pour les emails personnels, des logiciels privés ou le PC des enfants. C'est aussi un environnement où on recrée une situation pour tester des mises à jour, tester de nouveaux logiciels. »

Comprendre et agir sur les sept paliers d'une tentative de piratage

Bref, le lieu est idéal pour découvrir et maîtriser chacune des sept étapes d'une cyberattaque.

Sept étapes ? « Absolument », reprend Johan Helin. « C'est ce que nous appelons le « Cyber kill

chain ». Dans 95 % des cyberattaques, ce sont toujours les mêmes sept étapes qui se reproduisent. Apprendre à contrer ces attaques à chaque palier permet de renforcer la sécurité de son système.»

Un pirate commence généralement par effectuer une reconnaissance, une analyse du réseau qu'il veut prendre pour cible. Il élabore ensuite un scénario d'attaque (phase dite de « weaponization »). Commence ensuite l'intrusion à proprement parler avec l'identification d'une faiblesse dans le système. Et bien souvent, c'est une erreur humaine, de type hameçonnage (phishing) qui lui permet d'injecter ensuite son logiciel malicieux, de l'installer chez sa victime et enfin de l'activer pour arriver à ses fins : voler des données, bloquer le système, exiger une rançon, etc. « Toute la chaîne peut ne durer que quelques heures… ou s'étaler sur plusieurs mois », précise le spécialiste du Cyber Range de Transinne.

Le Centre de cybersécurité wallon est désormais en service et disponible. Des premières journées de formation ont déjà été organisées, notamment autour de la thématique de l'industrie 4.0 avec le concours du hub digital Walhub. L'offre du Centre de cybersécurité est vaste. À ce stade, 18 scénarios de base avec trois versions de difficultés sont disponibles.