LE NOUVEAU PARTENARIAT ENTRE LE GROUPE PRISME ET TEHTRIS SIGNE UNE NOUVELLE ÈRE DANS LA LUTTE CONTRE LES CYBER-MENACES

L'INTELLIGENCE ARTIFICIELLE SE MET AU SERVICE DE LA CYBERSÉCURITÉ AVEC LA NOUVELLE SOLUTION eGAMBIT TEHTRIS – GROUPE PRISME

Les Plans Hôpital 2008 et 2012, suivis par le Programme Hôpital Numérique, ont signé l'avènement de l'ère digitale dans les établissements de santé. Une transition dans laquelle se sont résolument engagés les acteurs sanitaires, conscients des nombreux atouts offerts par l'informatisation de la production de soins, la mise en œuvre de technologies d'acquisition automatique des données ou encore le déploiement d'équipements communicants. Mais la transformation numérique n'est pas exempte de risques : plus ouverts, les réseaux hospitaliers sont plus vulnérables aux cyber-attaques, logiciels de chantage et autres tentatives de piratages – autant de menaces protéiformes qu'il peut être difficile de contrer.

Une problématique désormais prise à bras le corps par le Groupe PRISME, titulaire du marché des solutions de traçabilité code-barres et de mobilité à l'UGAP. Cet intégrateur de solutions clés-en-main s'est en effet engagé dans un partenariat stratégique avec la start-up bordelaise TEHTRIS, dont la plateforme e-Gambit a obtenu le Label France Cybersécurité et les Trophées de l'Innovation IT 2016. Véritable cyber-arsenal défensif, e-Gambit sait détecter et parer à toutes les menaces, y compris celles non répertoriées par les logiciels experts. Une efficacité qui l'a vu rapidement séduire des entreprises du CAC40, et dont les établissements de santé ont aujourd'hui tout à gagner. Le point avec Bernard Rubinstein, président du Groupe PRISME, et Laurent Oudot, co-fondateur de TEHTRIS.

PAR JOËLLE HAYEK

Bernard Rubinstein, Président du Groupe PRISME

QUELS SONT LES PRINCIPAUX ENJEUX EN MATIÈRE DE SÉCURISATION DES SYSTÈMES D'INFORMATION (SSI) DANS LES ÉTABLISSEMENTS DE SANTÉ ?

BERNARD RUBINSTEIN : Il faudrait, pour mieux appréhender les différentes problématiques, commencer par rappeler les grands concepts de la sécurité de l'information. Celle-ci s'articule autour de trois notions principales : **la confidentialité**, définie par l'Organisation Internationale de Normalisation (ISO) comme le fait de s'assurer que les données ne sont accessibles qu'aux personnels habilités. Une nécessité d'autant plus prégnante dans le secteur sanitaire, où il est question de données sensibles à caractère personnel - leur divulgation pourrait donc porter préjudice au patient.

Deuxième grande notion, l'**intégrité**, qui permet de garantir la non altération des données lors de leur traitement, conservation ou transmission. C'est là un enjeu de taille pour les établissements de santé, puisque toute atteinte à l'intégrité des données médicales est susceptible d'entraîner des erreurs, voire un préjudice vital envers le patient – comment en effet définir une straté-

gie thérapeutique pertinente sur la base d'éléments ayant été intempestivement modifiés par un homme ou une machine ?

Troisième point, **la disponibilité de l'information**, pierre angulaire de la continuité des soins : les professionnels de santé doivent pouvoir accéder, en temps réel, aux données nécessaires à la prise en charge des patients. Une non disponibilité des données lors d'une intervention chirurgicale peut par exemple être source de retards ou d'erreurs, et cette méconnaissance du contexte médical peut se traduire par une perte de chance pour le patient. Citons pour finir l'imputabilité, ou la gestion des preuves, qui concerne tous les aspects de la SSI en permettant de tracer les actions et d'en identifier les auteurs.

COMMENT CETTE SÉCURITÉ DE L'INFORMATION SE DÉCLINE-T-ELLE AUJOURD'HUI SUR LE TERRAIN ?
LAURENT OUDOT : Forts de leur expertise technique, les directeurs des systèmes d'informations (DSI) sont sensibilisés aux différents enjeux de la SSI et tentent d'assurer leur mise en œuvre sur les réseaux et infrastructures. Ils y sont d'ailleurs fortement incités par l'Agence des Systèmes d'Information Partagés de Santé (ASIP Santé) et sa Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S). Mais il leur est difficile, sinon impossible, de sécuriser le SI dans son ensemble, compte-tenu de la pénétration de l'outil informatique dans tous les processus métier – ce qui multiplie d'autant les failles potentielles.

Par ailleurs, les établissements de santé sont de plus en plus nombreux à ouvrir leur SI vers la ville afin de faciliter les échanges avec les professionnels libéraux, voire à créer des portails patients pour que les usagers puissent être acteurs de leur propre parcours sanitaires. Bien qu'elles constituent un atout incontestable en matière de coordination des soins, ces évolutions augmentent la vulnérabilité du SI. Une tendance amenée à s'accélérer avec la récente constitution des Groupements Hospitaliers de Territoire (GHT) et la mise en œuvre de systèmes d'information communicants à l'échelle d'un bassin sanitaire.

Or, et c'est justement là le cœur du problème, les établissements de santé consacrent peu de ressources, financières ou physiques, à la cybersécurité – une étude publiée cette année a ainsi rapporté que le budget consacré à la sécurité des systèmes ne représentait que 6% du budget total dédié aux services informatiques dans les établissements de santé français. Focalisés sur l'informatisation de la production des soins, ces derniers ne sont pas suffisamment sensibilisés à l'importance de la cybersécurité, alors que ces deux notions sont étroitement liées ; les dysfonctionnements seraient en effet conséquents (effacement des données, dérèglement ou arrêts des appareils médicaux, etc.) si un hôpital venait à subir une cyber-attaque.

LES ÉTABLISSEMENTS DE SANTÉ REPRÉSENTENT-ILS UNE CIBLE POUR LES CYBER-PIRATES ?
LAURENT OUDOT : C'est même une cible de choix ! Non seulement leurs systèmes sont globalement vulnérables, mais la multiplicité des personnes ayant accès au SI permet d'y ouvrir facilement des « brèches ». La santé représente d'ailleurs un secteur stratégique pour les cyber-pirates : un éditeur d'antivirus s'est penché, cette année, sur l'intérêt qu'ont les hackers à s'attaquer aux hôpitaux ; l'on y apprend que les dossiers médicaux électroniques peuvent être vendus à 50 dollars l'unité sur le marché noir ! Par ailleurs, au vu de la criticité de l'activité hospitalière et de son niveau de dépendance vis-à-vis des outils informatiques,

Laurent Oudot, co-fondateur de TEHTRIS

le blocage des accès au système d'information est une activité tout à fait rentable pour les cyber-pirates. Mais la finalité de ces opérations n'est pas toujours matérielle : un hacker peut tout simplement être mal intentionné, et dérégler les équipements médicaux ou altérer des protocoles de soins pour son propre divertissement… Les menaces sont ▶

▶ donc multiples : ce peut être des attaques ciblées sur une personne ou un module en particulier, ou des attaques opportunistes qui multiplient les essais à moindre coût pour tenter de trouver les cibles les plus faibles ; des attaques basiques, qui s'appuient sur des vulnérabilités connues, ou des attaques sophistiquées ; elles peuvent être du fait d'un individu isolé, d'un groupe « mafieux », voire même d'un État aux ressources quasi-illimitées.

BERNARD RUBINSTEIN : Certaines attaques ont d'ailleurs été cette année sous les feux de l'actualité. Ainsi, en février dernier, le Hollywood Presbytarian Medical Center de Los Angeles, aux États-Unis, a été victime d'un « ransomware », ou logiciel de chantage, qui a ont été touchés par un logiciel de chantage. Plus proche de nous, plusieurs sources ont rapporté que l'hôpital Émile-Durkheim d'Épinal, dans les Vosges, aurait été victime d'un rançonnage informatique en mars 2016, tandis que l'hôpital Duchenne, à Boulogne-sur-Mer dans le Pas-de-Calais, a été ciblé par un ransomware à trois reprises en moins de quinze jours. Les hôpitaux français ne sont donc pas épargnés !

CE QUI NOUS AMÈNE JUSTEMENT À LA PLATEFORME eGAMBIT, MISE AU POINT PAR TEHTRIS ET DÉSORMAIS INTÉGRÉE AU PORTEFEUILLE DU GROUPE PRISME. DANS QUEL CONTEXTE CETTE SOLUTION A-T-ELLE VU LE JOUR ?

LAURENT OUDOT : eGambit s'inscrit, en quelque sorte, dans la continuité de mon parcours professionnel, ainsi que dans celui d'Elena Poincet, la cofondatrice de TEHTRIS. Anciens experts opérationnels de la Direction Générale de la Sécurité Extérieure au sein du Ministère de la Défense, nous avons été amenés à nous pencher sur les dangers liés à la cybersphère – constatant alors qu'il n'existait aucune certitude technique pour contrer des risques qui, eux, sont bien réels. Nous avons donc créé TEHTRIS en 2010, pour mettre notre expertise en matière de SSI à disposition de services étatiques (Organisation des Nations Unies, armée américaine, gouvernement d'Arabie Saoudite,…), de géants du Web (Google, Apple, Twitter), de constructeurs (BlackBerry, Intel) ou d'autres grandes entités.

« LES ÉTABLISSEMENTS DE SANTÉ CONSACRENT PEU DE RESSOURCES, FINANCIÈRES OU PHYSIQUES, À LA CYBERSÉCURITÉ – UNE ÉTUDE PUBLIÉE CETTE ANNÉE A AINSI RAPPORTÉ QUE LE BUDGET CONSACRÉ À LA SÉCURITÉ DES SYSTÈMES NE REPRÉSENTAIT QUE 6% DU BUDGET TOTAL DÉDIÉ AUX SERVICES INFORMATIQUES DANS LES ÉTABLISSEMENTS DE SANTÉ FRANÇAIS »

intégralement paralysé son système informatique ; après une dizaine de jours de statu quo, il s'est résigné à payer une rançon aux administrateurs du programme pour récupérer ses données – une mésaventure qui lui aura coûté un peu plus de 15 000 euros, alors que les pirates en réclamaient au départ 3,2 millions ! Un mois plus tard, MedStar Health, qui gère une dizaine d'hôpitaux dans le Maryland et la région de Washington D.C., était à son tour ciblé ; il a été contraint de désactiver son réseau, sans préciser si l'attaque était accompagnée d'une demande de rançon. Toujours en mars, deux hôpitaux californiens gérés par Prime Healthcare Services ont eux aussi dû fermer leur système, tandis que l'hôpital d'Ottawa, au Canada, a annoncé que quatre de ses ordinateurs

Les nombreux audits que nous y avons mené autour de la sécurité et des risques d'espionnage ont conforté notre constat initial : les produits disponibles sur le marché ne sont pas suffisamment efficaces pour détecter les risques de piratage. D'où la création de la plateforme e-Gambit, dont la première version a été dévoilée en octobre 2012. Elle a, en six mois, été adoptée par Michelin et Vallourec, deux entreprises cotées au CAC40, avant d'être déployée dans d'autres grandes infrastructures. En octobre 2015, ce cyber-arsenal défensif a obtenu le « Label France Cybersecurity », sous le haut patronage du gouvernement et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Il a en outre reçu le Trophée de l'Innovation en Sécurité Informatique lors du « IT Innovation Forum 2016 »,

un événement organisé sous le parrainage d'Axelle Lemaire, Secrétaire d'État chargée du numérique.

COMMENT FONCTIONNE PLUS PRÉCISÉMENT LA PLATEFORME eGAMBIT ?

LAURENT OUDOT : Celle-ci offre une cybersurveillance et une cyberprotection opérationnelles complètes, à travers la création d'un serveur virtuel local (Cloud) associé à des cybergardiens, qui surveillent l'ensemble des flux et communiquent, de manière sécurisée, avec le serveur central de TEHTRIS. Plus concrètement, le serveur local eGambit écoute l'ensemble des signaux, qu'ils soient forts ou faibles, et les interprète en temps réel. La solution effectue par exemple des analyses heuristiques, c'est-à-dire ciblées sur le comportement d'un programme, pour déterminer s'il s'agit ou non d'une menace. Autant de données qui sont ensuite remontées dans le serveur central et corrélées aux autres informations dont nous disposons – une vue unifiée qui nous permet de savoir si une opération de piratage est en cours et d'activer, au besoin, le système d'alarme de cybersécurité.

BERNARD RUBINSTEIN : Le Groupe PRISME est résolument engagé pour la French Tech, et nous apprécions le fait que les technologies utilisées par TEHTRIS soient 100% françaises et assurément innovantes – intelligence artificielle, capteurs de détection avancées, etc. Modulable, eGambit est par ailleurs en mesure de répondre à tous types de besoins de nos clients publics et privés, tant au niveau de la plateforme d'alarme cybersécurité, que des cyber-gardiens chargés de superviser

« LA MULTIPLICITÉ DES PERSONNES AYANT ACCÈS AU S.I. HOSPITALIER PERMET D'Y OUVRIR FACILEMENT DES « BRÈCHES »

la sécurité informatique à distance. Elle a en outre deux autres grandes forces : son déploiement est simple et rapide, et son administration informatique est pleinement assumée à distance par TEHTRIS, évitant aux sites équipés de mobiliser leurs ressources internes. Un avantage incontestable pour les établissements de santé, où les effectifs ne sont pas toujours en adéquation avec les besoins réels – et les compétences pas toujours disponibles puisque, à l'exception notable des CHU, rares sont les hôpitaux à disposer d'un Responsable de la Sécurité des Systèmes d'Information (RSSI). Pour plus de lisibilité, l'offre désormais proposée au catalogue UGAP a été découpée en modules, afin que les établissements de ▶

CYBERMENACES DANS LES HÔPITAUX FRANÇAIS : PAROLES D'EXPERT

Responsable de la Sécurité des Systèmes d'Information (RSSI) au CHU de Nantes Pays de Loire, Cédric Cartau est notamment l'auteur de *La sécurité du système d'information des établissements de santé*, seul ouvrage traitant, à ce jour, de la SSI en établissement de soins. Interrogé par nos confrères du Monde en février dernier, suite au ransomware dont avait été victime le Hollywood Presbytarian Medical Center de Los Angeles, il dresse un état des lieux réaliste de la cybersécurité dans les établissements de santé : « *Il y a environ mille hôpitaux en France, mais à peine cinquante responsables sécurité des systèmes d'information. La situation n'est pas plus enviable dans les structures privées, et c'est encore pire dans le médico-social. Dans 95 % des cas, il n'y a personne pour se préoccuper de sécurité informatique* ».

Dans le même article, Vincent Trély, le président de l'Association pour la promotion de la sécurité des systèmes d'information de santé (APSSIS), estimait que de nombreux établissements de santé français ont subi des tentatives d'extorsion de ce genre, même si celles-ci ne sont pas médiatisées : «*Toutes les semaines, je suis informé d'un ou deux cas. Mais Il y a une sorte d'omerta sur le sujet, ce qui est compréhensible, les établissements de santé ne sachant pas trop comment communiquer sur ce problème. Et ils ne souhaitent sans doute pas le faire* ».

« *La question n'est pas de savoir si l'attaque aura lieu mais quand elle interviendra et de s'y préparer* », rappelait pour sa part Nathalie Devillier, Professeur de droit à la Grenoble École de Management, dans un article publié sur The Conversation. En effet, « *l'explosion du big data dans tous les domaines, en particulier celui de la santé avec l'e-santé, la télémédecine, les milliers d'apps de suivi médical ou de bien-être augmentent l'exposition au risque de cyberattaque [pour les] établissements de santé* [et les] *patients* ». Et d'enfoncer le clou : « *Les enjeux de telles attaques sont particulièrement critiques dans le domaine de la santé en raison du caractère stratégique des informations auxquelles les soignants ont accès* ». Pourtant, souligne-t-elle, « dans 90% des cas, les hackers ont utilisé des vulnérabilités identifiées en interne (gestion des patch, firewalls, malware, antivirus) mais non traitées malgré la gravité des conséquences de ces potentielles failles ».

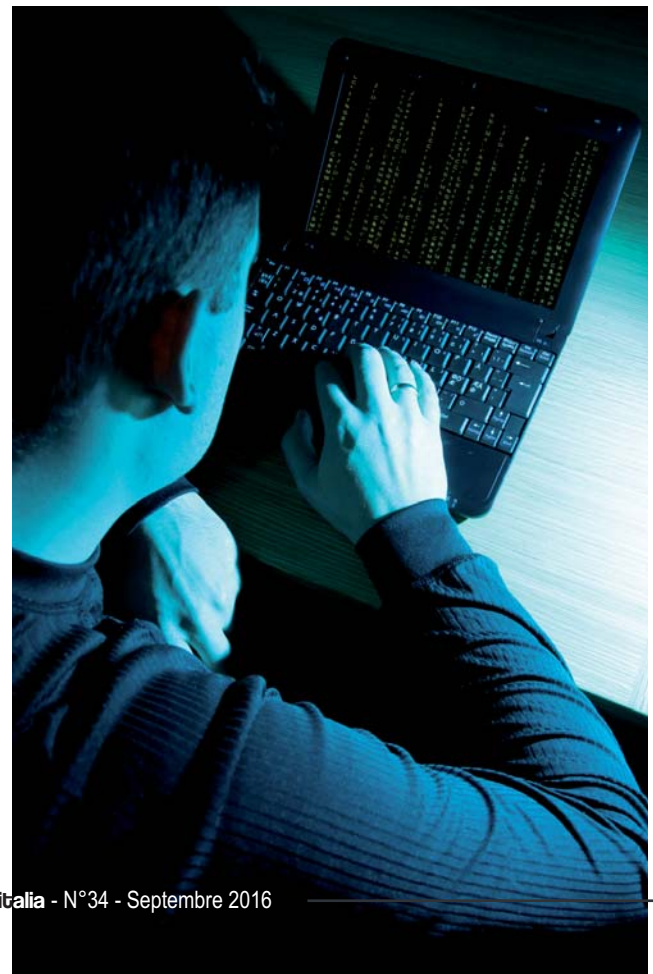
Sources :
https://theconversation.com/cyber-crime-sante-et-big-data-pirates-aujourdhui-corsaires-ou-flibustiers-demain-56699
http://www.lemonde.fr/pixels/article/2016/02/24/des-hopitaux-francais-eux-aussi-victimes-de-chantage-informatique_4870885_4408996.html

« COMPTE-TENU DE LA RECRUDESCENCE DES MENACES SÉCURITAIRES, LE GROUPE PRISME TRAVAILLE DEPUIS PLUS DE DEUX ANS DÉJÀ POUR CONCEVOIR ET DÉPLOYER UN PORTEFEUILLE DE SOLUTIONS DE SÉCURITÉ PUBLIQUE, ET A INTÉGRÉ RÉCEMMENT UNE SOLUTION COMPLÈTE DE TRAÇABILITÉ DES ENTRÉES ET SORTIES DANS LES BÂTIMENTS, EN PARTENARIAT AVEC LA SOCIÉTÉ WINKHAUS »

▶ santé puissent aisement disposer de solutions clés-en-mains, en adéquation avec leurs besoins techniques.

Ces modules sont répertoriés ci-dessous :

• Vérification des traces par un expert TEHTRIS : entre 1h et 7h /jour ouvré, ou surveillance et analyse des évènements critiques 24h/24 et 7j/7 toute l'année, avec alerte en cas d'intrusion avérée et analyse manuelle par une sentinelle TEHTRIS. C'est le Service eGambit.



• Surveillance Activités Systèmes : Traçabilité des actions techniques et réalisation d'investigations. Centralisation des traces sur le serveur eGambit et corrélations, avec en option l'ajout d'une source de logs eGambit.

• Surveillance Activités Réseaux : Suivi des échanges automatisés, identification des menaces et failles de sécurité. Détection des intrusions par signatures, autopsies des flux réseaux, audits passifs continus.

• Surveillance Zone : Suivi tactique des infrastructures pour les zones nécessitant une gamme avancée de capteurs. Inventaire du parc, leurres informatiques (honeypots), audits et autopsies post cyber-intrusions.

• Protection des Stations et Serveurs : Lutte contre les attaques furtives ou violentes, avec le serveur virtuel de gestion des agents eGambit Endpoint Security pour Windows et Linux. En option, ajout d'un un agent eGambit déployé sous Windows ou Linux.

• Option Haute Disponibilité eGambit : Serveur virtuel de secours.

• Prestations de service et d'expertise eGambit : conseil et expertise en traçabilité anti-intrusion et en cyber-sécurité eGambit à distance : pré-études, études spécifiques, gouvernance, services techniques, gestion des cybercrises.

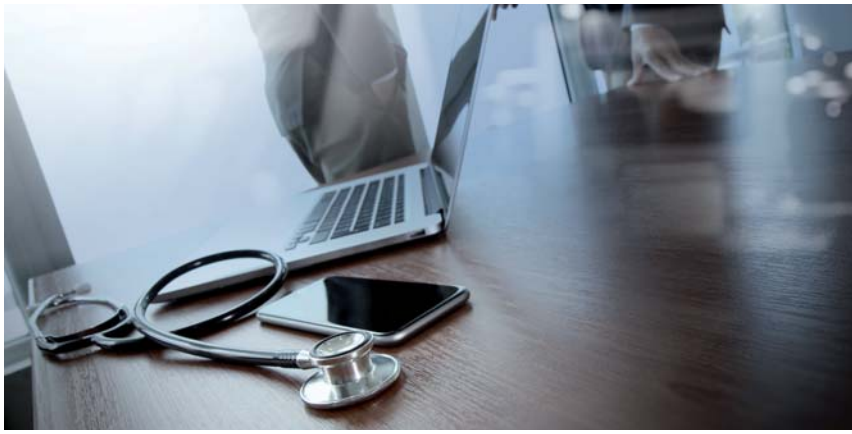
ARRÊTONS-NOUS POUR FINIR SUR CE PARTENARIAT ENTRE LE GROUPE PRISME ET TEHTRIS. POURQUOI CE RAPPROCHEMENT ?

BERNARD RUBINSTEIN : Ce partenariat est stratégique et s'inscrit au cœur de nos activités. Il fait en effet écho aux compétences métier développées par le Groupe PRISME dans les domaines de la traçabilité, des réseaux informatiques et de la mobilité, dans un contexte de convergence technologique, et de besoins clients toujours plus intégrés

et à forte valeur ajoutée technologique. Le Groupe PRISME a développé une expertise reconnue au niveau de la sécurisé des réseaux sans fil, du développement applicatif en mobilité, et de la réalisation d'interconnexions entre applications mobiles sur PDA et systèmes centraux (ERP, WMS, SIH, …). Cette expertise a d'ailleurs permis au Groupe PRISME obtenir les certifications les plus élevées dans les domaines *Wireless security, Congerged communication, Wireless local area networks, Wireless outdoor networks*, et également RFID. Alliant traçabilité des échanges et protection des données, ce savoir-faire s'est traduit par le déploiement chez nos clients de solutions complètes intégrant Wi-Fi, logiciels embarqués, matériel code-barres/RFID, ainsi que les services et prestations associés.

À la demande de nos clients publics et privés, notre catalogue a par la suite été étendu afin d'offrir des réponses pertinentes aux enjeux de sécurité publiques auxquels ils sont aujourd'hui confrontés. Compte-tenu de la recrudescence des menaces sécuritaires, le Groupe PRISME travaille depuis plus de deux ans déjà pour concevoir et déployer un portefeuille de solutions de sécurité publique, et a intégré récemment une solution complète de traçabilité des entrées et sorties dans les bâtiments, en partenariat avec la société WINKHAUS. Cette solution s'appuie sur le chiffrement AES 128 bits, reconnu comme l'un des algorithmes de cryptage les plus sécuritaires à ce jour et utilisé pour les échanges classés confidentiels défense en France comme aux États-Unis, l'utilisation de clés électroniques, et la création de réseaux virtuels permettant de prévenir toute intrusion par une diffusion virale des informations concernant les attaques en temps réel.

Le Groupe PRISME a pour vocation de répondre aux besoins actuels de ses clients acteurs publics, et également d'anticiper leurs besoins émergents. Nous avons par conséquent été amenés à travailler sur les problématiques des cyber-menaces et des ransomware, et c'est dans ce contexte que nous avons choisi de développer un partenariat avec l'une des sociétés les plus innovantes dans ce domaine : les algorithmes mis au point par TEHTRIS font en effet la part belle à l'intelligence artificielle pour assurer la cyber-surveillance et la cyber-protection des données. La solution eGambit s'inscrit donc dans le prolongement direct de notre cœur de métier qui, rappelons-le, consiste à assurer la traçabilité des flux physiques et des flux d'informations associés. Cette solution de cyber sécurité 100% française – c'est important pour nous – est en outre désormais disponible au catalogue UGAP.



LAURENT OUDOT : Si TEHTRIS bénéficie d'une expertise incontestable en matière de cyber-protection, le Groupe PRISME dispose quant à lui d'atouts de taille : son niveau de compétences technologiques et sa base de clientèle. Il a une forte présence dans le secteur public, où il a été associé à des projets ambitieux dans les administrations centrales, les communautés d'agglomération, les brigades de sapeurs-pompiers, les universités et musées, sans oublier plusieurs centaines d'hôpitaux et nombre d'établissements sanitaires et sociaux. Le Groupe PRISME a également une base conséquente de clients dans le secteur privé, notamment dans les domaines du transport et de la logistique, de la distribution et de l'industrie. Autant de partenaires avec lesquels il a su construire des relations de confiance sur la durée, et qui sont ou peuvent être légitimement intéressés par les solutions que nous avons développées. Ce rapprochement permet donc à TEHTRIS de s'associer avec un acteur majeur dans les domaines de la traçabilité, de la mobilité et des réseaux, dont le haut niveau de compétences techniques nous permet d'échanger de manière pratique et concrète autour des enjeux en matière de cybersécurité. Une synergie dont devraient bénéficier les établissements de santé, les producteurs de soins et les patients ! ■

«CETTE SOLUTION DE CYBER SÉCURITÉ 100% FRANÇAISE – C'EST IMPORTANT POUR NOUS – PROPOSÉE PAR LE GROUPE PRISME EST EN OUTRE DÉSORMAIS DISPONIBLE AU CATALOGUE UGAP»