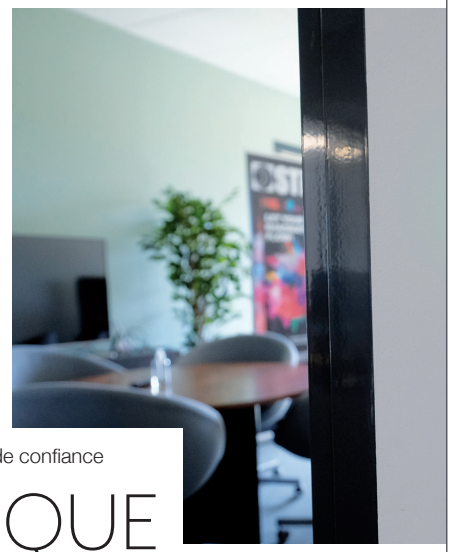
Article
La sécurité physique et la sécurité digitale sont intimement liées

Hospitalia - N°53 - Mai 2021



STid : sécuriser les accès et les identités avec des technologies de confiance

« LA SÉCURITÉ PHYSIQUE ET LA SÉCURITÉ DIGITALE **SONT INTIMEMENT LIÉES** »

Par Pamela Claude / Leader français des technologies instinctives sans contact, STid développe des solutions de gestion des accès et des identités hautement sécurisées pour les secteurs les plus exigeants. Cette PME basée à Gréasque, dans les Bouches-du-Rhône, est notamment reconnue pour ses systèmes évolutifs et ergonomiques basés sur des technologies ouvertes, comme nous l'expliquent Vincent et Baptiste Dupart, respectivement PDG et Responsable de Développement chez STid.

Pourriez-vous, pour commencer, nous présenter STid ?
Vincent Dupart : STid a été créé en 1996 afin de protéger les actifs stratégiques des entreprises, c'est-à-dire les personnes, les biens et, de plus en plus, les données. Nous adressons cet objectif à travers deux activités historiques, la sûreté et la traçabilité. Sur le premier champ, STid est aujourd'hui le premier fabricant français de systèmes de contrôle des identités et accès physiques. Nous ambitionnons de devenir le premier fabricant européen d'ici cinq ans, ce qui nous positionnera comme le principal concurrent du numéro un mondial, un constructeur nord-américain. Il faut dire que nous avons ici un certain nombre d'atouts.

Justement, cela fait plusieurs années que vous militez pour la généralisation des technologies dites « de confiance ». Qu'entendez-vous par là ?
Vincent Dupart : Les systèmes de contrôle d'accès sont en effet traditionnellement basés sur des technologies propriétaires. Avec STid, nos clients restent autonomes et maîtres de leur sécurité grâce à des technologies ouvertes et évolutives. Nous offrons une sécurité forte reposant sur des protocoles de communication standardisés comme le protocole SSCP® certifié CSPN par l'ANSSI, et synonyme de liberté, d'interopérabilité et de réactivité face aux menaces. Ce combat pour l'adoption à grande échelle de ces technologies de confiance est aujourd'hui devenu stratégique, en particulier en France et en Europe où il est désormais question d'atteindre la souveraineté européenne en matière de sécurité d'ici 2025. Nous accompagnons et sensibilisons les directions de sûreté des entreprises, y compris dans les établissements de santé, à ces nouveaux enjeux.

Comment comptez-vous porter ce message ?
Vincent Dupart : En 2020, nous avons créé l'alliance S.P.A.C., un syndicat professionnel qui fédère à ce jour une trentaine d'acteurs français et européens, tous engagés dans la promotion des technologies de confiance. Cette initiative est d'ailleurs soutenue par l'ANSSI, l'Agence Nationale pour la Sécurité des Systèmes d'Information, qui en est l'un des membres fondateurs et qui va œuvrer pour construire une industrie de la Sécurité, forte et ouverte. S.P.A.C. proposera une offre de certification fonctionnelle avec le protocole SSCP® pour garantir des solutions interopérables et fortes.

Article
La sécurité physique et la sécurité digitale sont intimement liées

Hospitalia - N°53 - Mai 2021

Vincent Dupart, PDG et **Baptiste Dupart,**
Responsable de Développement chez STid

« STID S'ATTACHE À DÉVELOPPER DES MODES D'IDENTIFICATION FLUIDES AFIN DE **SUPPRIMER LES CONTRAINTES POUR LES UTILISATEURS ET RENFORCER LEUR ADHÉSION À LA POLITIQUE DE SÉCURITÉ** »

C'est que l'enjeu va au-delà de la filtration des accès physiques. Vous évoquiez plus haut la sécurisation des données. Pourriez-vous nous en parler ?
Vincent Dupart : La sécurité physique et la sécurité digitale sont en effet intimement liées : un système de sécurisation des accès est non seulement connecté au système d'information, mais les identifiants sont eux-mêmes de plus en plus dématérialisés, avec notamment l'utilisation des Smartphones. Dans les entreprises, les Directeurs de Sûreté sont d'ailleurs en train de converger avec les Responsables de la Sécurité et des Systèmes d'Information, et cette tendance devrait progressivement arriver à l'Hôpital. Un autre exemple : sans système de contrôle des accès efficace, une personne malveillante peut aisément copier un badge à la volée – ce qui est beaucoup plus facile qu'on ne le croit –, pénétrer dans le local des serveurs informatiques et compromettre les données. D'où la nécessité de migrer vers des technologies sûres et pérennes, mais aussi ergonomiques. C'est pourquoi STid s'attache, aussi, à développer des modes d'identification fluides afin de supprimer les contraintes pour les utilisateurs et renforcer leur adhésion à la politique de sécurité.

Quel regard portez-vous aujourd'hui sur la sécurisation des accès au sein des établissements de santé ?
Baptiste Dupart : Nous sommes régulièrement sollicités pour des audits et constatons, bien souvent, que les technologies en place sont quelque peu dépassées. Les failles de sécurité sont donc potentiellement nombreuses. Il faut dire que les établissements de santé ont un certain nombre de contraintes, sur le plan de l'exploitation, des budgets, de la continuité de service… sans oublier une masse salariale parfois conséquente, avec plusieurs milliers d'utilisateurs à équiper.

Comment répondez-vous à ces enjeux ?
Baptiste Dupart : Nous commençons toujours par évaluer le parc existant et les besoins réels pour préconiser une stratégie de migration la plus simple possible. Nous préconisons généralement un plan très progressif, avec dans un premier temps une technologie refuge puis une technologie cible, afin de ne pas remettre en question tout le système. La gamme Architect® garantit justement une migration douce, que l'on choisisse de commencer par les badges ou les lecteurs. Tous deux sont en effet bi-technologiques : on peut continuer d'exploiter la technologie précédente le temps que la transition soit complète, tout en fonctionnant sur la technologie de nouvelle génération. L'établissement peut alors disposer, à terme, d'une solution de gestion des accès parfaitement sécurisée, y compris en matière de communication avec un système tiers, sans qu'il ne soit nécessaire de faire également évoluer ses logiciels. Autre point important : les lecteurs Architect® sont basés sur une technologie normée et 100% compatible avec les nouvelles cartes de professionnels de santé et d'établissements (CPSx, CPE, CPx).

Par la suite, si le besoin évolue, l'établissement de santé a l'assurance que ses badges et lecteurs STid resteront compatibles. C'est tout le principe des technologies de confiance que nous évoquions plus haut, et qui recouvrent *in fine* plusieurs notions : fiabilité, évolutivité, ergonomie, interopérabilité, modularité, indépendance, autonomie… Autant de valeurs que nous portons depuis notre création.

Plus d'informations :
www. stid-security.com