

Article

Réglementations, normes, certifications, qualifications, labels : passeports vers le marché

INFOPROTECTION - Newsletter - Juin 2019

Rendre la sécurité visible sur les produits, créer la confiance chez les partenaires, s'assurer que les produits de sécurité résistent aux cyberattaques... la notoriété des produits réclame de construire une forte reconnaissance par des organismes à la légitimité indiscutable.

A l'instar du Règlement européen sur la protection des données personnelles (RGPD) qui s'est appliqué depuis le 25 mai 2018 dans tous les États-membres de l'UE, les normes réglementaires sont imposées par les autorités administratives de haut niveau. Mais à côté de ces règlements ou normes réglementaires, les normes volontaires, les marques et les certifications prolifèrent. Avantage : elles créent la confiance. En témoigne Rémi Bréval, directeur produit chez Genetec, l'éditeur canadien de la plateforme unifiée de sécurité Security Center lors du salon Expoprotection 2018 : « La certification, en l'occurrence la Certification de Sécurité de Premier Niveau (CSPN) du niveau IV, la plus élevée que délivre l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui porte sur notre automate Security Center Synergis Cloud Link, prouve qu'il répond aux standards de cybersécurité et de sécurité physique parmi les plus élevés en Europe. »

Normes volontaires

Les normes volontaires sont issues des instituts de normalisation. Comme Afnor en France, British Standard Institute (BSI) au Royaume-Uni, Deutsches Institut für Normung e.V. en Allemagne, Asociación Española de Normalización y Certificación (Espagne), Ente Nazionale Italiano di Unificazione ou, au niveau européen, Comité européen de normalisation (CEN), Comité européen de normalisation électrotechnique (Cenelec), European Telecommunications Standards Institute (ETSI) ou encore le European Computer Manufacturers Association (ECMA). Ces instituts ont tous en commun d'encadrer les normes volontaires qui ont pour objectif d'établir un cadre de référence avec des prescriptions techniques ou qualitatives concernant des produits, services ou pratiques. Elles sont déterminées par les fabricants, les installateurs et les utilisateurs. Tout le monde peut proposer un projet de norme, toutes les parties concernées par le projet sont alors entendues avant de passer à l'homologation de la norme c'est-à-dire sa validation.



Labels : des marques plus ou moins sérieuses

Les labels (ou marques) sont définis par des signes distinctifs : un nom, un logo et un cahier des charges à respecter. Attention, les labels peuvent être attribués par des organismes privés et publics, certains sont donc plus fiables que d'autres. Préférez les labels délivrés par des organismes reconnus avec vérification par un tiers. Citons la marque A2P qui porte sur la résistance des serrures, des portes et blocs-portes de bâtiment à l'effraction et aux cambriolages. Ce label de qualité est délivré par le Centre national de prévention et de protection (CNPP Cert.), l'organisme de certification officiel reconnu par les professionnels de l'assurance.

Article

Réglementations, normes, certifications, qualifications, labels : passeports vers le marché

INFOPROTECTION - Newsletter - Juin 2019

Certifications : un processus parfois très complexe

En revanche, la certification est une démarche visant à faire reconnaître la qualité et la conformité des produits et des services. Délivrée par un organisme certificateur indépendant, la procédure comprend un audit et une phase de tests. Elle permet d'être plus visible étant fiable (audit, test et contrôle périodique) et signalée par un logo. C'est un véritable gage de qualité. Mais ce processus peut être plus complexe. C'est le cas de la certification A2P qui est effectuée par un comité d'attribution qui réunit des syndicats de fabricants et de distributeurs comme l'Union nationale des industries de la quincaillerie (UNIQ), l'organisation professionnelle représentatives des concepteurs, fabricants et installateurs de menuiseries aluminium (SNFA) ou le Syndicat national des fabricants de menuiseries industrielles (SNFMI). Ainsi que des représentants des organismes de consommateurs désignés par le Conseil national de la consommation (CNC) : l'Assemblée plénière des sociétés d'assurances dommages dont la marque APSAD (sécurité incendie) est délivrée par CNPP Cert.), la Fédération des chambres pharmaceutiques de France (FCPF), la Fédération des chambres syndicales des horlogers-bijoutiers (FCSHB). En outre, on y retrouve également des représentants de l'Association financière des banques (AFB) et des organismes à forte compétence : Afnor, le Centre d'expertise du bâtiment et des travaux publics (CEBTP), le CNPP, la Fédération des industries mécaniques et transformatrices de métaux (FIMTM), l'Institut national de la consommation (INC). Ainsi que des représentants des pouvoirs publics : la direction des assurances du ministère de l'Économie et des Finances, ministère de l'Intérieur, ministère de la Recherche... Ce comité délivre la marque A2P suivant les procès-verbaux et les rapports du CNPP.



La marque A2P bénéficie d'une certification délivrée par un comité. © CNPP



Ce lecteur et son protocole de communication ont été les premiers à recevoir la certification CSPN de l'ANSSI. © STid

accès physiques. » Figurant parmi les participants à ce groupe, STid a été le premier constructeur à recevoir, dès 2013, la fameuse Certification de sécurité de premier niveau (CSPN) de l'ANSSI. Bien sûr, la CSPN démontre la fiabilité du système non seulement auprès des clients mais aussi des partenaires qui intègrent cette technologie au sein de leurs solutions.

Certificat de sécurité de premier niveau (CSPN)

Pendant, les choses se sont complexifiées avec la sécurité électronique, cible des cyberattaques. Outre les caméras de vidéosurveillance, qui ont été le point d'entrée de rançongiciels comme Wannacry, Petya, NoPetya ou Industroyer, les systèmes sans fil de contrôle d'accès ont également révélé leur besoin de sécurisation. « Avant 2012, plusieurs failles de sécurité affectant les technologies sans contact sont avérées, explique Nicolas Roussel, directeur marketing de STid, un des leaders du contrôle d'accès. Un groupe de travail interministériel, animé par l'ANSSI, a évalué que les conséquences de ces failles étaient particulièrement préoccupantes lorsque les technologies sans contact étaient utilisées dans les systèmes de contrôle des