Le Label ExpertCyber, une brique indispensable pour la confiance et la sécurité numériques

Franck GICQUEL
Responsable des partenariats
Cybermalveillance.gouv.fr

Pour assurer la sécurité numérique de son entreprise, de sa collectivité ou de son association, il est indispensable d'intégrer et de concilier les ressources humaines et techniques bien en amont. Trop souvent négligé ou considéré comme non prioritaire, le facteur « humain » est une composante essentielle de la chaîne de sécurisation. Largement exposé aux menaces et démultipliant, par conséquent, la surface d'attaque des cybercriminels qui en profitent pour commettre leurs forfaits à peu de frais, il doit être suffisamment sensibilisé aux risques numériques et formé aux bonnes pratiques. Il contribuera, ainsi, et de façon proactive, au renforcement de la sécurité informatique de sa structure en devenant lui-même un « capteur du terrain », capable d'alerter en cas de problème et, ainsi, de contribuer à la prévention des incidents. Le volet technique, quant à lui, doit, par essence, permettre de renforcer son système d'information, afin de faire face aux attaques toujours plus ingénieuses, sophistiquées, et en constante progression technologique.

Ce sont principalement les grandes organisations qui maîtrisent de mieux en mieux ces deux volets ; elles possèdent en effet des équipements robustes et disposent des ressources internes dédiées, couplées à des prestataires informatiques bien identifiés. Ainsi, lorsque celles-ci sont la cible de cybercriminels, elles sont mieux armées face aux attaques. S'agissant des plus petites structures, en revanche, le constat est malheureusement bien différent. D'après l'analyse des plus de 200 000 demandes d'assistance recensées sur la plateforme Cybermalveillance.gouv.fr depuis sa création en 2017, 12 % concernent les parcours des professionnels (dont les collectivités et les associations). Ces derniers ont eu recours à Cybermalveillance.gouv.fr pour bénéficier de conseils de première urgence ou de l'assistance technique d'un professionnel de proximité référencé sur la plateforme. Peu équipées, par manque de moyens ou d'informations sur les risques numériques, les victimes constatent trop tard la faible sécurité mise en place au sein du système informatique de leur structure, mettant sérieusement en danger leur activité.

Il est donc indispensable de se faire accompagner par des professionnels pour assurer une sécurisation des systèmes bien en amont et se prémunir ainsi contre les risques numériques. Mais alors, vers quels acteurs de confiance se tourner lorsque l'on est une TPE-PME ou une petite collectivité ? Avec le nombre important de sociétés informatiques sur le marché, sur la base de quels critères faire son choix ? Comment s'assurer de la qualité ou de la compétence d'un professionnel ?

Ce sont les questions auxquelles Cybermalveillance.gouv.fr a souhaité répondre, en lançant fin 2018 un groupe de travail composé des principaux syndicats et fédérations de prestataires de services numériques, membres du dispositif Cybermalveillance.gouv.fr : Cinov Numérique, Fédération EBEN, Syntec Numérique et la Fédération Française de l'Assurance (FFA). Cette dernière a été associée à la réflexion avec son statut d'interlocutrice de proximité des assureurs et des mises en relation qu'elle peut effectuer entre ses assurés et des prestataires de services de toutes natures, dont le numérique. L'objectif de ce groupe de travail était de réfléchir et de proposer des solutions pour répondre au besoin des utilisateurs de se sécuriser en amont par des professionnels de confiance ayant démontré leur niveau de compétences techniques.

La collaboration avec des prestataires de services en sécurité informatique était déjà au cœur de l'action du dispositif et ce, depuis sa création, mais uniquement sur le volet « post-incident ». En effet, Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels qui contribuent activement à sa mission d'assistance aux victimes. Les particuliers, entreprises et collectivités victimes d'actes malveillants sur Internet peuvent ainsi se connecter à la plateforme www.cybermalveillance.gouv.fr pour obtenir un diagnostic de leur situation et des recommandations sur les problèmes rencontrés. Concrètement, en suivant un parcours en ligne au travers de quelques questions simples, ils sont conseillés et, le cas échéant, mis en relation avec un réseau de près 1 000 professionnels, répartis sur l'ensemble du territoire. C'est notamment grâce aux retours de ces professionnels en sécurité numérique que l'enrichissement de l'outil de diagnostic et la mise à jour des conseils sont rendus possibles. Les profils des professionnels référencés sont très hétérogènes (domaines d'intervention, taille, publics ciblés...), ce qui permet d'être en capacité d'apporter à tout individu ou organisation, une assistance technique qualifiée partout en France. Cela est d'autant plus important pour des entreprises, collectivités et associations victimes d'incidents plus complexes, parfois avec des informations très sensibles en jeu. C'est grâce à l'ensemble de ce réseau présent sur le terrain et en contact avec les publics que nous pouvons apporter une réponse aussi large.

Face à cette grande diversité, et en l'absence d'un « label » dédié aux professionnels en sécurité numérique s'adressant spécifiquement aux publics professionnels (TPE-PME, collectivités et associations), il était nécessaire de reconnaître et valoriser un nouveau niveau de réponse en termes d'expertise et de périmètres. C'est ainsi qu'est né le Label ExpertCyber. Ce label a été créé pour plusieurs raisons, en premier lieu, pour apporter aux utilisateurs une meilleure lisibilité de la qualité d'offre de service, condition nécessaire pour créer un climat de confiance dans le numérique, mais également pour valoriser et aider les prestataires justifiants d'un certain niveau d'expertise en sécurité numérique, et inciter à la montée en compétence. Il était aussi devenu très vite évident durant la phase de conception que le Label ExpertCyber ne pouvait se limiter à l'assistance post-incident. Pour cette raison, décision fut prise d'élargir les périmètres d'action à l'installation et la maintenance afin d'être en capacité de fournir aux entreprises et aux collectivités un accompagnement global sur le volet préventif.

Sur le dispositif de labellisation, le dispositif a opté pour un audit documentaire couplé à un questionnaire technique. Les audits sont menés par l'AFNOR, organisme professionnel de la certification, qui a accompagné le groupe de travail durant toute la démarche afin de valider le niveau d'expertise attendu des candidats. Les auditeurs se basent sur un référentiel qui regroupe un ensemble d'exigences couvrant quatre principaux domaines : les compétences techniques, la qualité de service client, la conformité administrative et le sens de l'intérêt général. Bien que constitutive de l'ADN du label, ce n'est donc pas uniquement l'expertise technique qui est évaluée, mais un ensemble de caractéristiques qui

renforce la chaîne de confiance, notamment pour des publics souvent peu aguerris sur le sujet de la sécurité numérique, voire sur le numérique tout court.

Le label ExpertCyber sera lancé publiquement au début de l'année 2021 et aura pour ambition de contribuer à l'amélioration et au renforcement du niveau de sécurité des entreprises, des collectivités et des associations en favorisant leur mise en relation avec des acteurs de confiance. Elle sera possible depuis un nouveau service dédié sur la plateforme Cybermalveillance.gouv.fr et également accessible au travers d'autres outils, afin que ce nouveau label puisse profiter au plus grand nombre.