Stimuler les dynamiques organisationnelles avec le Security by Design

Parce qu'elle porte en elle des problématiques techniques, juridiques ou encore contractuelles, cette approche est nécessairement organisationnelle. La notion de "Security by Design" est donc à diffuser dans tous les pans de l'entreprise, de façon à ce qu'elle irrigue chaque prise de décision.
Cela exige notamment d'adapter son modèle organisationnel ainsi que son approche projet.

Patience est mère de Prudence

« La patience est une vertue » pourrait être le mantra de toute personne cherchant à mettre la sécurité au cœur de son organisation. En effet, trop souvent, l'erreur couramment commise est ainsi de voir « trop grand » et de vouloir aller « trop vite ». Chercher à mettre de la sécurité à tous les niveaux et simultanément, sans avoir, au préalable, pris le temps de s'informer sur les spécificités des différents métiers de l'entreprise, c'est se diriger droit vers l'échec. Le risque est ainsi de se retrouver avec des procédures et dispositifs à la fois coûteux et inopérants, puisque inadaptés et non adoptés par les équipes.

On peut démarrer facilement en choisissant les premiers projets naissants et en évaluant les périmètres concernés. Cette phase initiale sera l'occasion d'affiner son organisation, d'identifier les bonnes et mauvaises pratiques, de lever les problèmes. Il sera ensuite plus facile d'industrialiser cette approche et de la rendre pilotable. Au fur et à mesure que l'expertise sécurité se répandra dans l'organisation, de plus en plus de projets pourront être menés en parallèle.

La sécurité passe l'épreuve de la certification

En lançant la démarche organisationnelle "Security by Design", il est important de considérer l'objectif de faire certifier sa démarche. En effet, le déclaratif pèse toujours moins lourd dans la balance décisionnelle que la preuve de la certification par un tiers indépendant.
L'entreprise a donc tout intérêt à faire auditer – par un tiers de confiance – sa stratégie en matière de sécurité. Non seulement cela va l'obliger à définir un contexte, à réfléchir aux risques et à la façon de les gérer, mais ce sera aussi la meilleure garantie possible à apporter à ses clients, ses partenaires et ses investisseurs.

Certes, la certification représente un investissement, mais ce dernier sera largement compensé par l'impact positif que la certification aura sur les décisions business des clients.
Enfin, il faut savoir faire preuve de transparence, en étant toujours à l'écoute et en laissant ses

clients se rendre compte par eux-mêmes des procédures mises en place pour garantir la sécurité de leurs données.

Parvenir à créer « un réflexe sécurité »

Infuser la culture du risque dans l'entreprise, c'est aussi identifier dans chaque équipe, les personnes ayant de l'appétence pour ce sujet. Elles deviendront des « DevSecOps » : des référents sécurité qui interviendront au plus proche des équipes dans chaque Business Unit. En devenant les relais de la stratégie « Security By Design » au quotidien, elles participeront pleinement à l'acculturation de tous.
Cela ne s'envisage toutefois qu'en rendant les collaboratrices et collaborateurs plus responsables de leurs actes. Il faut leur donner envie de s'investir et d'expérimenter la notion de « Security By Design ». Ils doivent apprendre à se poser les bonnes questions avant chaque prise de décisions, comme par exemple : « Suis-je en conformité avec les règles de sécurité de mon entreprise ? », « Ai-je besoin de l'accompagnement d'un expert sur ce sujet ? »… Ce questionnement doit devenir un automatisme, que ce soit dans le cadre de l'installation d'un nouveau logiciel sur son ordinateur ou lors de la création d'un nouveau produit.

Mieux prévenir, c'est mieux guérir

Pour autant, inutile d'asséner des dogmes en matière de sécurité. L'entreprise doit laisser une part de libre arbitre à ses collaboratrices et collaborateurs, tout en mettant à leur disposition les bons outils pour accompagner leurs prises de décisions. Ces supports serviront avant tout à construire la conformité organisationnelle, mais le plus important sera la capacité des salariés à prendre en compte le risque. L'anticipation de ce dernier permettra d'imaginer la riposte la plus adaptée.

Rappelons toutefois que le risque zéro n'existe pas. Il y aura toujours des vulnérabilités techniques ou humaines. Une stratégie « Security by Design » sert surtout à apporter les moyens de mieux anticiper le risque, d'être prêt à le contrer et d'en limiter les conséquences au maximum.