AVIS
D'EXPERT

Quand la sécurité devient un levier compétitif

Incontournable et coûteuse, la sécurité a longtemps été considérée comme une « simple » nécessité liée aux risques et aux usages. Ce n'est plus vrai. La cybersécurité devient une réponse nécessaire aux menaces et plonge désormais au cœur des produits ou des processus de l'entreprise : un changement que l'entreprise peut et doit transformer en avantage compétitif.

On a l'habitude de voir la sécurité comme un passage obligé qui coûte cher à mettre en place. Or, absente ou défaillante, elle risque de coûter encore plus à l'entreprise. A cet égard, les faits sont impressionnants : attaque par phishing sur TV5 Monde, vol de plusieurs milliards de dollars dans une centaine de banques via le malware Carbanak et ce dans plus de 30 pays, fuite de données et déni de service chez Sony ou attaque sur le fabricant de jouets VTech… Des épisodes qui traduisent une augmentation spectaculaire de la cybercriminalité à l'échelle mondiale. Verizon estime son coût à 400 milliards d'euros en 2014 !

Pourtant, là n'est (presque) pas le plus important. Un changement profond est en train de se produire : la perception et la place même de la sécurité dans l'entreprise et dans son écosystème évoluent.

Développer la confiance numérique

Certes, une lacune de sécurité peut détruire de la valeur par la perte de données ou une atteinte à la notoriété avec des conséquences majeures, car les impacts potentiels sont nombreux : sur le fonctionnement (missions en cours, capacité de décision), sur les hommes (sécurité des personnes, lien social interne), sur les biens (patrimoine intellectuel ou culturel, finances, image), sans compter les impacts juridiques, de non-conformité ou sur l'environnement.

Mais c'est ailleurs que la sécurité va trouver son véritable essor : elle s'inscrit désormais dans un mouvement profond de « confiance numérique » alors que le « marketing de la confiance » commence à voir le jour. Véritable facilitateur de transformation numérique, la cybersécurité permet de créer de nouveaux produits ou services qui auront d'emblée la confiance des utilisateurs ou des actuels ou futurs consommateurs, et apporte ainsi un avantage concurrentiel.

De façon plus générale, la confiance favorise les échanges, et donc la création de valeur au sein des services et des produits. A l'instar de l'économie réelle, la perte liée à la mise en place de frontières numériques se traduirait par des coûts complémentaires, avec une répercussion sur la compétitivité, et une baisse des échanges ou d'adoption des produits.

Apporter plus de confiance, c'est créer moins de risques, moins de coûts, et développer ainsi de nouveaux avantages compétitifs.

« La cybersécurité passe du statut de « nécessité » coûteuse à celui de levier de compétitivité par la création de nouveaux produits ou de nouveaux services. »

Sécurité et nouveaux vecteurs de valeur

Concrètement, comment positionner la confiance dans le business model de l'entreprise pour en faire un avantage concurrentiel ? Trois vecteurs de valeur s'imposent alors.

1. Introduire la sécurité dans les produits et ses services

La sécurité est de plus en plus présente au cœur même des produits innovants, qui créent autant de nouveaux risques pour l'entreprise ou le consommateur : les objets connectés, les produits basés sur la technologie NFC, etc. Autant d'innovations qui ne seraient pas viables sans une sécurité native.

Prenons l'exemple type d'un nouveau produit compétitif. Avec les protocoles de sécurité renforcés des cartes de paiement sans contact, le risque est réduit, la confiance des utilisateurs élevée et la valeur du produit accrue. Ainsi, le taux d'adoption a augmenté et les banques tendent à acquérir le marché des petits montants (de moins de 20 €), même si le développement en France reste faible eu égard au marché.

2. Introduire plus de sécurité dans les procesus

Dans un contexte d'entreprise étendue, les rapports entre les acteurs nécessitent un haut niveau de confiance numérique. L'amélioration des réseaux de confiance permet de mieux collaborer pour fiabiliser les échanges de données. La cybersécurité permet à une entreprise de raffermir ses processus, comme par exemple dans la supply chain ou dans les relations entre un industriel et ses sous-traitants PME (automobile, aéronautique, etc.) : la compétitivité par la confiance numérique s'en trouvera accrue par un meilleur partage des données, tout en limitant les risques. Il en est de même pour la relation entre les banques.

Le pôle de compétitivité Aerospace Valley a ainsi labellisé des projets de cybersécurité pour l'Aérospatial visant à fédérer à la fois les entreprises des secteurs aéronautique et spatial européens et les travaux de recherche des centres de formation. L'objectif est de mieux appréhender les enjeux de la sécurité de l'ensemble de la filière, et de proposer aux PME et aux ETI des solutions abordables répondant à leurs besoins.

3. L'enjeu majeur des compétences en sécurité

Afin de garantir la confiance envers les nouveaux produits ou services liés aux nouveaux usages du numérique, la surveillance doit être formalisée pour détecter en amont et mieux réagir en cas d'attaque : la confiance passe par le contrôle. Sur un marché pénurique de la cybersécurité, l'enjeu de la compétence et de la spécialisation dans ce domaine est clé. La cybersécurité se dote actuellement de compétences liées au big data et machine learning afin d'améliorer la qualité de la détection de la menace.

L'évolution de l'économie numérique place la cybersécurité à la fois comme une nécessité pour les entreprises et comme un élément de différenciation. Cette valeur doit être créée sur l'ensemble de la chaîne de service des entreprises, dans une logique de sécurité globale. Pour devenir opérateur de confiance, celles-ci sont de plus en plus amenées à construire des relations partenariales avec des offreurs globaux en sécurité, spécialistes dans leur domaine. Cette tendance se trouve renforcée par les obligations légales issues notamment de la loi de programmation militaire et des règlementations européennes.

Auteur

Florent Halbot
est Directeur Adjoint de la Division Cybersécurité de Sopra Steria. Ses domaines d'expertises sont étendus, tant à la fois sectoriels, métiers et technologiques.
Après un début de carrière dans les réseaux, la sécurité et l'expertise judiciaire au sein des Ministères de la Défense et de la Justice, il a notamment accompagné l'opérateur télécom Prosodie dans sa transformation et la mise en place d'un nouveau positionnement d'opérateur transactionnel et hautement sécurisé. Florent Halbot est diplômé de Polytechnique promotion 1987.

Sopra Steria - Direction Communication & Marketing
contact-corp@soprasteria.com

www.soprasteria.com