Big Data, une sécurité lacunaire ?

Dépérimétrisation : le néologisme est lancé, aussi barbare qu'abyssal. Il indique un décloisonnement du système d'information et sans périmètre précis, la donnée peut être créée, captée, traitée, modifiée, stockée n'importe où, n'importe quand.

La dépérimétrisation offre dès lors un monde des possibles gigantesque, aidé de données riches (structurées, non-structurées, multimédia…), polymorphes et multi-provenances, à la croissance exponentielle encore accélérée par les objets connectés, du plus petit capteur de réseau à la voiture intelligente et connectée.

Attention toutefois derrière cette « nébuleuse » apparente de données, les supports physiques demeurent (y compris ceux sans fil, car bien qu'utilisant le principe des ondes radio, immatérielles, ceux-ci demeurent des supports physiques). Dans ce contexte, au même titre que la matière, il est possible de caractériser les données selon trois états : les données au repos (état solide) sur des disques de stockage, les données en transit (état liquide) sur les réseaux, et les données en traitement (état gazeux) sur des serveurs.

Cette analogie pédagogique permet de comprendre le lien entre les données, leurs supports physiques selon leurs états respectifs et la sécurisation qui doit en découler, sur l'ensemble du cycle de vie des données.

Sécuriser la donnée, y compris lors de son traitement

Reconnue comme un véritable actif de l'entreprise depuis longtemps, la donnée bénéficie d'une attention particulière quant à sa protection. En matière de stockage, sa confidentialité et son intégrité sont le plus souvent assurées par des contrôles d'accès (physiques et logiques), du chiffrement et d'autres mécanismes de cloisonnement entre disques, machines virtuelles, processus, etc.

De la même façon, la sécurité protocolaire (IPSEC sur IP, TLS sur http ou WPA2 ou 3 sur WiFi, etc.) assure la protection des données lorsqu'elles sont en transit. Avec une attention toute particulière portée sur les réseaux sans fil, tant il est aisé « d'écouter » les flux qui n'y seraient pas protégés.

Lorsqu'elle est en traitement, la donnée est aussi particulièrement vulnérable. Sa protection est d'autant plus difficile à appréhender dans ce contexte qu'elle implique également les programmes chargés de son traitement. Le risque étant qu'une modification malveillante du programme pourrait entraîner une action qui n'aurait pas lieu d'être ; par exemple, un véhicule qui ne freine pas alors qu'il le devrait (ou l'inverse).

Dès lors, c'est toute l'intégrité du programme, sa configuration et son intelligence (IA) qui doivent être préservées pour assurer la sécurité de la donnée.

La sécurité des IoT, premier rempart

Avec la multiplication des appareils digitaux et la connectivité apportée à des objets qui ne l'étaient pas précédemment, tels que des véhicules, des réfrigérateurs, et même des chaînes de production, les données sont donc bien partout désormais : c'est même autour de ces objets que la donnée est bien souvent captée et digitalisée, et parfois restituée.

Extérieurs au système d'information par définition, les objets connectés représentent en outre une surface d'attaque colossale, avec autant de portes d'entrée potentielles vers les données des organisations. Ils sont donc les premiers éléments à sécuriser pour limiter les risques de malveillance, en particulier dans les secteurs stratégiques, impactant la santé humaine ou aux enjeux économiques particulièrement importants.

C'est évidemment le cas de l'automobile, du médical (santé connectée), des grands réseaux et Opérateurs d'Importance Vitale (eau, électricité, télécommunications, armée/défense), et de toutes les grandes industries dont les arrêts de production sont économiquement dramatiques.

Pour toutes ces activités en particulier, mais également pour l'ensemble de l'économie, seul un niveau de sécurité intégré et homogène de bout en bout, depuis les objets connectés jusqu'aux profondeurs du Cloud, permettra d'assurer la sécurité d'un monde où la donnée est partout.

Le défi est donc aujourd'hui de penser à une sécurité unifiée avec des politiques (mise à la clé, maintenance, réaction en cas d'attaque) coordonnées et des technologies corrélées entre elles, afin d'obtenir des niveaux d'assurance homogènes, quel que soit l'état de la donnée (solide/liquide/gazeux).

Une sécurité qui doit également bénéficier d'une meilleure orchestration, face à une chaîne de valeur de la sécurité aujourd'hui très fragmentée et à l'absence à ce jour d'acteur en charge du métier spécifique d'opérateur de sécurité, qui superviserait cette chaîne de valeur et en assumerait la « liability ».

Enfin, et dans un contexte de souveraineté, des technologies permettant une gestion systémique de la sécurité doivent émerger. Le contexte est propice (EU cyber act) et la vision stratégique désormais comprise de l'écosystème. A nous d'agir !