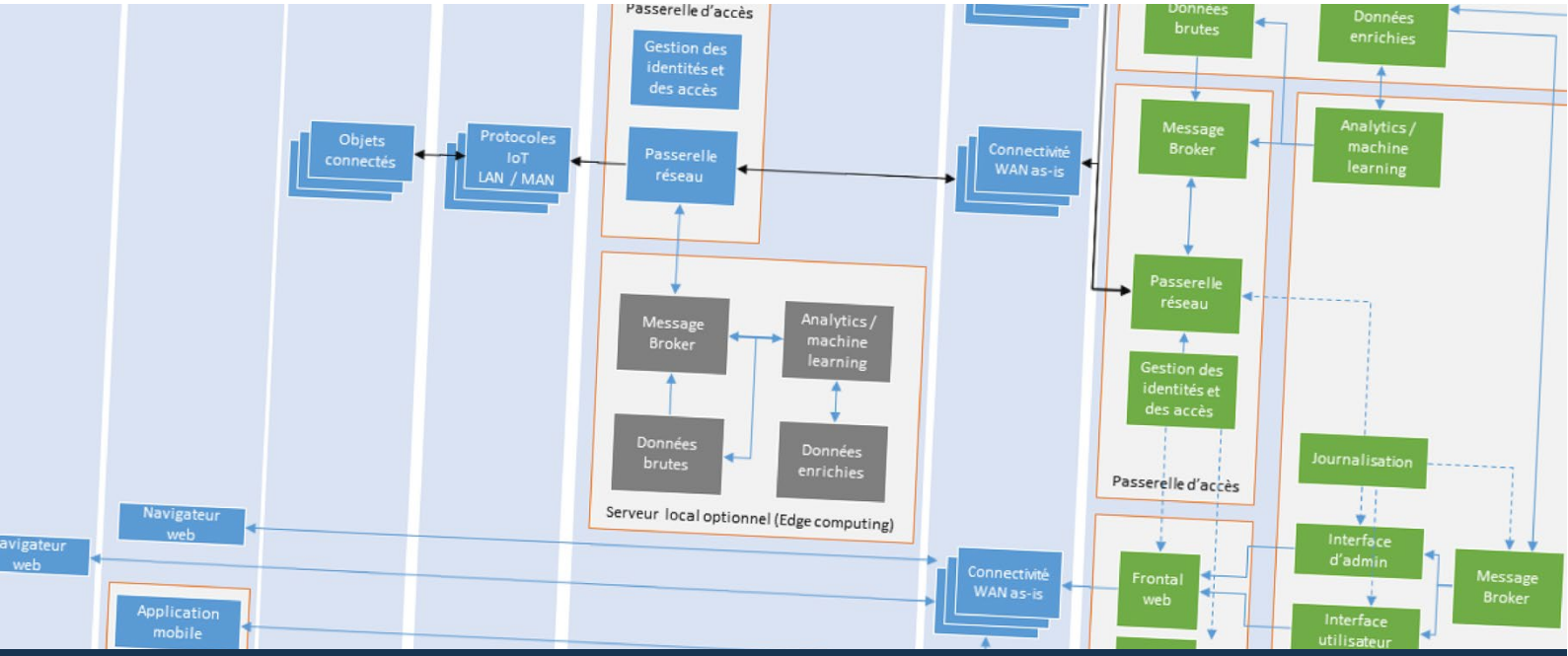
LES FICHES PRATIQUES du CLUSIF - IoT



Pourquoi les RSSI devraient s'intéresser au sujet dès maintenant ?

Version 1.0

1. IoT et transformation numérique

L'IoT a été un moteur de la transformation numérique qui s'est produite ces dernières années dans des organisations du monde entier. Le scénario d'innovation autour de la nouvelle gamme d'objets connectés et la production et la consommation massives de données provenant de ceux-ci ont contribué de manière significative à l'émergence d'une nouvelle variété de cas d'utilisation innovants. En outre, la valeur des données générées par le nombre croissant d'objets a débloqué une nouvelle gamme d'opportunités commerciales pour de nombreux segments de l'industrie. Ce scénario impose de nouveaux défis technologiques et de gouvernance qui devraient être inclus dans l'ordre du jour du RSSI, où des sujets tels que la gestion des objets, la confidentialité des données et la sécurité par conception sont obligatoires.

L'identification et le traitement des nouvelles exigences de sécurité découlant de l'adoption accélérée de nouvelles technologies IoT constituent l'un des principaux rôles et l'un des principaux défis des RSSI, nécessitant un processus d'apprentissage et de développement continu. Pour relever ces défis sans ralentir le processus d'innovation, les RSSI et ses équipes doivent plus que jamais travailler au sein de la DSI, devenant un acteur actif de la transformation numérique de son entreprise.

2. Quelques chiffres importants

Les nouvelles opportunités commerciales générées par l'IoT ont augmenté le montant des investissements dans le secteur, comme le montrent les prévisions de Gartner dans le tableau 1.

Avec une base installée de plus de 20 milliards d'unités d'IoT estimées d'ici 2020, Gartner estime également à près de 3 000 milliards de dollars les dépenses liées aux terminaux IoT la même année.

Ce montant d'investissement peut potentiellement mener à une forte concurrence sur différents segments de marché, où la réduction des délais de mise sur le marché constituera un élément essentiel de la stratégie commerciale pour devenir un leader du marché, mais contribuera également au développement d'une posture de sécurité inappropriée. En plus de ce scénario, Gartner estime à seulement 2,5 millions de dollars les dépenses consacrées à la sécurité de l'Internet des objets en 2020, ce qui ne représente que 0,08% des dépenses consacrées aux terminaux IoT pour la même année.

	2017	2018	2020
Base installée des unités IoT par catégorie (en millions d'unités)	8 380	11 196	20 415
Dépenses liées aux terminaux IoT par catégorie (en millions de dollars)	1 689 572	2 094 881	2 925 787
Prévision mondiale des dépenses de sécurité de l'IoT (en millions de dollars)	1 174	1 506	2 457

Tableau 1 - Prévisions pour le marché IoT. (Sources : Gartner January 2017 [i] and March 2018[ii]).

En regard de ces chiffres il faut prendre en considération les enjeux financiers associés à la sécurité informatique à commencer par les risques d'amende pour non-respect des réglementations comme le RGPD. Ces chiffres doivent aussi conduire les professionnels de la sécurité à envisager un scénario pessimiste dans lequel ils devraient faire face à une situation critique associée à des problèmes de sécurité des objets connectés déjà déployés. De plus, compte tenu des caractéristiques hautement évolutives et distribuées des systèmes IoT, nous pouvons nous attendre à des problèmes de sécurité encore plus importants que ceux observés actuellement pour les systèmes IT / OT existants. Plus qu'une tendance du marché, ces prévisions doivent être considérées comme une alerte sur les défis futurs en matière de sécurité IoT, qui nécessitent une attention immédiate des RSSI pour établir les bases de compétences, de gouvernance et d'infrastructure qui soutiendront les actions futures.

3. Comment construire des solutions IoT résilientes et évolutives ?

En choisissant de suivre les tendances de l'innovation IoT, les RSSI peuvent ne pas être en mesure d'éviter le scénario pessimiste prévu, mais ils seront certainement en mesure d'atténuer leur impact commercial et d'agir selon une approche plus structurée et plus fiable. Bien que le nombre de déploiements IoT en production augmente chaque jour, principalement grâce à la large gamme d'objets, de technologies de réseaux et de plates-formes cloud émergentes, le marché est toujours à la recherche de normes largement acceptées par la communauté, de bonnes pratiques et de directives.

Cela représente une opportunité unique pour les RSSI de se rapprocher de la conception et de la spécification de solutions IoT innovantes et d'influencer activement la posture de sécurité des équipes de projet en favorisant l'adoption de pratiques et de technologies de sécurité appropriées.

4. Normes et réglementations

Les normes de cyber sécurité ont joué un rôle très important dans la diffusion des meilleures pratiques dans différents segments de l'industrie, tandis que les réglementations imposent des mesures appropriées contre les risques susceptibles d'avoir un impact direct ou indirect sur la société. Bien qu'elle soit à un rythme accéléré d'innovation, l'industrie de l'IoT est toujours à la recherche de normes et de réglementations spécifiques susceptibles d'assurer l'application des meilleures pratiques et le respect des normes existantes, liées à la sécurité mais aussi à l'interopérabilité et à d'autres exigences pertinentes. À partir de l'analyse de l'état actuel des initiatives de normalisation de l'IoT, nous pouvons observer que la plupart des travaux existants sont axés sur la définition et les spécifications fonctionnelles des technologies IoT, avec peu ou pas d'attention aux aspects de sécurité. Par ailleurs, les organisations de cybersécurité du monde entier ont élaboré des recommandations de sécurité et des meilleures pratiques pour l'IoT visant à combler les lacunes existantes. Nous pouvons citer en particulier le document « Recommandations de base sur la sécurité pour l'IoT[iii] » de l'ENISA.

Étant donné le niveau de maturité de l'industrie de l'IoT, ainsi que le processus complexe et le temps requis par les organismes internationaux de normalisation, le RSSI a pour rôle d'observer les recommandations actuelles des organisations de sécurité crédibles et de fournir des normes internes pour soutenir les projets innovants mis en œuvre par l'IoT.

Parallèlement, les réglementations actuelles, telles que le RGPD et la directive NIS, peuvent avoir un impact considérable sur la sécurité de l'IoT. Le développement croissant des systèmes IoT pour les objets personnels attire l'attention sur la confidentialité des informations traitées par ces objets, qui sont la plupart du temps limités en ressources et qui n'implémentent pas les fonctionnalités de sécurité appropriées.
La loi Californienne « *Information Privacy : Connected Devices* [iv]» constitue un premier embryon de cadre officiel qui rentre en vigueur le premier janvier 2020 qui demande aux constructeurs d'implémenter des mesures de sécurité raisonnables dans tous les objets connectés distribués en Californie. Ces mesures ne sont pas précisées dans le détail et doivent être adaptées selon la nature et les fonctionnalités des objets connectés, en particulier les informations collectées stockées ou transmises. Néanmoins cette loi impose aux constructeurs IoT de mettre en place pour chaque objet connecté un mot de passe unique ou un mécanisme imposant à l'utilisateur de créer un nouveau moyen d'authentification personnel avant toute utilisation de l'objet connecté.

5. L'impact dans l'entreprise

En outre, dans le cadre du déploiement en entreprise la connexion de nouveaux objets entraîne l'extension du périmètre de sécurité de la société. Cela affecte également la conformité aux normes en vigueur et aux certifications associées, telles que les standards ISO 27000, qui restent une des priorités des RSSI. Par conséquent, nous concluons qu'il est également de la responsabilité actuelle des RSSI d'inclure l'IoT dans leurs processus de gestion de la sécurité, afin d'avoir une visibilité complète de leur périmètre de sécurité et de s'assurer de la conformité de l'entreprise.

6. À quoi l'IoT peut servir pour améliorer la sécurité dans les entreprises ?

En supposant que le déploiement sécurisé des objets connectés peut être réalisé, la façon d'utiliser ces objets pour améliorer la sécurité des autres applications est encore un domaine sous-exploré. Cette section a pour but d'élargir les questions autour du paradigme de l'IoT au-delà de l'émergence de nouvelles surfaces de menaces et d'attirer l'attention des RSSI et autres rôles de sécurité sur la possibilité d'utiliser l'IoT pour améliorer la posture de sécurité actuelle de leur entreprise.

Les dispositifs IoT sont généralement déployés d'une manière qui leur permet d'interagir avec le monde physique afin d'exécuter des fonctions telles que la mesure, l'action et le contrôle. Une telle caractéristique place les dispositifs IoT dans une position stratégique pour permettre des solutions innovantes de sécurité et de sûreté pour les systèmes cyber-physiques. Parmi les objectifs de sécurité qui peuvent être atteints, nous soulignons la surveillance et l'alerte, ainsi que la redondance des mécanismes de sûreté. Alors que les capteurs joueront un rôle clé dans les mécanismes de surveillance et d'alerte, les contrôleurs et les actionneurs joueront un rôle clé dans la mise en œuvre des mécanismes de sûreté.
À titre d'exemple des systèmes de surveillance et d'alerte rendus possibles par l'IoT, on peut citer l'utilisation de caméras thermiques reliées à des systèmes analytiques capables de détecter des anomalies dans la signature thermique des équipements, processus ou sites critiques. Dans cet exemple particulier, les fonctions analytiques en question pourraient également être exécutées partiellement ou complètement par la caméra thermique, selon le niveau d'intelligence qui y est intégré. La détection d'une anomalie peut déclencher une alerte, voire une chaîne d'actions complexe en s'intégrant à d'autres systèmes de contrôle et de surveillance qui peuvent être en place.
Un deuxième exemple qui illustre comment l'IoT peut rendre possible la mise en œuvre de mécanismes de sécurité efficaces est l'utilisation d'un système de localisation en intérieur pour désactiver les processus ou équipements critiques en l'absence d'un membre du personnel responsable dans l'environnement opérationnel. Un tel système peut constituer le mécanisme de sûreté principal ou redondant en place pour un certain processus critique.
Divers autres exemples de systèmes de surveillance, d'alerte et de sécurité basés sur des objets intelligents connectés s'appliqueraient ici, en particulier ceux liés à la surveillance de sites ou d'équipements déployés dans des endroits éloignés ou d'autres d'accès limité. L'avènement de nouvelles technologies de connectivité, comme le LPWAN (*Low Power WAN*), a considérablement amélioré notre capacité à détecter et à réagir rapidement aux événements de sécurité qui se produisent dans des endroits où les opérateurs ne sont pas facilement disponibles, comme dans certaines lignes de production et de distribution d'énergie ou dans les infrastructures sous-marines.
Bien que l'utilisation d'appareils connectés à des fins de surveillance et de sécurité ne soit pas nouvelle, principalement dans les applications industrielles, l'avènement de nouveaux appareils plus intelligents et de nouvelles technologies de connectivité ouvrent les portes à une nouvelle gamme d'applications qui peuvent fonctionner avec un niveau élevé d'autonomie et de capacité analytique pour améliorer la sûreté et la sécurité des systèmes existants.

ⓘ Point de vue du RSSI

En conclusion, pour une exploitation durable de l'IoT il est important que les RSSI s'impliquent dans ces projets dès leurs premières phases car il sera difficile d'améliorer le niveau de sécurité d'un objet une fois qu'il aura été mis sur le marché. Cette fiche a pris le point de vue du RSSI mais les aspects de protection des données nécessitent que l'on implique également le DPO (Data Privacy Officer) dans cette réflexion globale. [v]

[i] https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
[ii] https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018
[iii] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
[iv] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327
[v] Voir en particulier la fiche de FAQ IoT CLUSIF qui aborde la collecte massive des données

LES FICHES PRATIQUES

L'intégralité de la FAQ IoT et la liste des membres qui ont contribué à son élaboration sont consultables sur le site du CLUSIF : **www.clusif.fr/publications**

CLUSIF