BIG DATA et Internet des objets

Outre le "Big Data", l'Internet des objets - en anglais, "Internet of Things" (IoT) - est l'une des principales questions d'avenir de l'informatique. Dans ce dossier, BEE SECURE explique le lien entre Big Data et IoT, comment ces deux phénomènes interagissent et les dangers et les chances qui en résultent.

Qu'est-ce que l'Internet des objets ?

Le terme "Internet des objets" (IoT) paraît abstrait et un peu bizarre, mais est vite expliqué : quand on parle d'Internet des objets, on parle d'appareils ou "d'objets" connectés à Internet. N'existe-t-il pas déjà de nombreux "objets", tels qu'ordinateurs, ordinateurs portables, smartphones, consoles de jeux, etc. qui sont connectés à Internet ?
En ce qui concerne l'IoT, il ne s'agit pas en premier lieu d'ordinateurs ou de téléphones portables, mais avant tout d'objets du quotidien, tels que réfrigérateurs, lampes, serrures, jeux et même brosses à dents.
Selon des estimations de l'institut d'études de marché Gartner, en 2017, 8,4 millions d'objets connectés étaient en ligne, 31 pourcents de plus que 2016. A l'horizon 2020, on s'attend à 20,4 millions appareils connectés à Internet.

Quels sont les exemples d'IoT ?

Les exemples les plus connus d'IoT actuellement sont sûrement les "assistants numériques", tels que Alexa de Amazon ou Home de Google. Apple aussi est en train de développer un appareil similaire qui se base sur "Siri". Les appareils sont des enceintes avec microphones intégrés qui réagissent à des commandes vocales et sont connectés au cloud. Grâce à ces assistants, il est non seulement possible d'accéder à des prévisions météorologiques ou d'écouter de la musique, ils peuvent également être connectés à d'autres appareils connectés. Il est ainsi possible d'allumer et d'éteindre via commande vocale la lumière d'ampoules "intelligentes" connectées.
D'autres applications sont par exemple les thermostats qui permettent de régler le chauffage également à distance - si vous débauchez plus tôt, vous pourrez allumer le chauffage pendant votre trajet. Les prises d'alimentation connectées permettent quant à elles d'allumer et d'éteindre les appareils "bêtes" via Internet. Certaines ampoules connectées, qui ont déjà été mentionnées, peuvent non seulement être allumées et éteintes via une application, mais créer également différentes ambiances de lumière. Il existe également des "smart locks", des serrures intelligentes, qui peuvent être déverrouillées via le smartphone. Ceux qui se soucient de la sécurité de leur maison peuvent s'équiper de systèmes de surveillance avec caméra et alarme - ou un capteur qui détecte précocement certains dangers, tels qu'incendie ou fuite d'eau.
L'IoT a non seulement trouvé sa place dans les ménages : dans le secteur de la médecine et du sport, il existe depuis un certain temps des bracelets qui collectent des données via les utilisateurs pour contrôler leur état de santé actuel. On trouve également des brosses à dents connectées sur le marché.

Sans oublier le secteur de la gestion du trafic : bus, trains, voitures, feux de signalisation, routes, etc. sont de plus en plus souvent équipés de capteurs et deviennent ce que l'on appelle des "Smart Cities". L'IoT permet d'obtenir une meilleure interaction des différents moyens de transport et un trafic plus fluide. Les avions et les bateaux aussi collectent un grand nombre de données - ainsi, un avion qui détecte un petit défaut peut être pris en charge immédiatement après son atterrissage.

Quand on pense aux vaches et aux prés, on ne pense pas forcément à l'IoT - et pourtant, l'agriculture a de plus en plus recours au numérique. Les agriculteurs peuvent ainsi vérifier sur votre ordinateur si les champs ont été arrosés ainsi que les différents volumes de lait produits par les différentes vaches, permettant de détecter d'éventuels signes de maladie. Des moissonneuses-batteuses, qui préviennent les agriculteurs d'orages et passent donc du mode économique à la puissance maximale, sont déjà utilisées.

Machine à café et Internet

La toute première webcam a été installée en 1991 à l'Université de Cambridge. Cela, pour pouvoir vérifier s'il restait du café dans la machine à café dans la salle de repos. Pouvoir afficher un carré en blanc et noir de 128 pixels nécessitait à l'époque un dispositif conséquent : une caméra, un ordinateur et une connexion à Internet. Aujourd'hui, il existe des machines à café qui peuvent être télécommandées par application via Internet. Chose inimaginable pour les chercheurs à Cambridge au début des années 90 !

Deux progrès techniques importants et essentiels à l'IoT ont rendu possible ce développement : la connectivité et l'adressable.

La connectivité est facile à expliquer : sans câbles, il est aujourd'hui possible d'intégrer à quasiment tous les appareils une puce WiFi ou une carte SIM. Pour les appareils pour lesquels cela n'est pas possible, il existe d'autres technologies, tels que Bluetooth ou communication en champ proche (NFC ou puces RFID, par exemple lors du paiement sans contact par carte bancaire).

L'adressabilité est un autre problème, plutôt de nature mathématique. Vous avez probablement déjà entendu parler de "adresse IP". Sur Internet (IP pour "Internet protocole"), chaque appareil a besoin d'une adresse, qui lui est attribuée de manière équivoque - comme chaque téléphone a son propre numéro de téléphone. Il y a quelques années encore, l'IPv4 (la version 4 de IP) a été utilisée, un format composé d'un numéro de 32 bits, par exemple "172.16.254.1." Cependant, il n'existe que 4,2 milliards d'adresses IPv4 – pas assez pour tous les appareils du monde. Heureusement, dès 1995 le successeur a été développé : IPv6 Cette version utilise des adresses longues codées sur 128 bits, comme par exemple : "2001:db8:0:1234:0:567:8:1" (les deux exemples sont d'ailleurs la même adresse). Avec cette version, 2^{128} adresses différentes sont possibles - 340 milliards milliards milliards milliards, un nombre de 39 chiffres. On obtient ainsi suffisamment d'adresse à très long terme.

Qu'en est-il du Big Data ?

Peut-être y avez-vous déjà pensé : si l'on trouve partout des appareils connectés à Internet, il doit y avoir un très grand nombre de données. Selon la société américaine Cisco, en 2018, l'IoT généra 400 zettaoctets de données. En 2013, il s'agissait de seulement 3,12 zettaoctets. Si l'on gravait cette quantité de données sur des DVD, on nécessiterait 10 milliards de disques.

Pour pouvoir utiliser ces énormes montagnes de données, des centres de données qui enregistrent et analysent les données sont nécessaires - et bien évidemment les bons algorithmes de Big Data. Le "Big" dans Big Data ne se rapporte toutefois pas seulement au volume des données, mais également à la vitesse, avec laquelle elles sont générées, et aux différents types de données : du goût musical des utilisateurs de "Alexa" en passant par la fréquence cardiaque d'un utilisateur de bracelet de fitness, à l'état de santé des vaches connectées.

Ces données sont collectées et ensuite intégrées aux banques de données. Pour cela, elles doivent être partiellement converties et corrigées des erreurs de mesure. Ces processus aussi peuvent aujourd'hui être assurés par des algorithmes.

Plus tard, les données sont traitées de sorte qu'elles soient également comprises par les êtres humains, par exemple dans des graphiques ou des cartes. Une "smart city" peut par exemple créer une vue d'ensemble des routes embouteillées, des feux de signalisation en panne et des quartiers où la qualité de l'aire est particulièrement bonne ou mauvaise.
Pour certains cas d'application, les données doivent être traitées très vite : par exemple pour les alarmes de sécurité ou les bracelets de fitness, qui surveillent p.ex. le rythme cardiaque d'une personne. Pour cette raison, certains appareils connectés peuvent eux-mêmes assurer une partie de l'analyse.

Sinon : toutes les données collectées sont, dans le doute, sauvegardées quelque part et attendent leur analyse.
Les applications possibles pour les données IoT, qui sont analysées à l'aide de méthodes Big Data, renferment un potentiel énorme : une agriculture plus efficace, qui utilise moins d'eau, moins d'engrais et moins de pesticide, une détection précoce des maladies, un meilleur système de transport, des logements automatisés, qui prennent en compte les besoins de leurs habitants etc. Les possibilités semblent sans limite, mais comme pour toute technologie, l'Internet des objets représente aussi beaucoup de dangers et de risques.

Mon grille-pain, un espion ?

Quand des appareils collectent des données sur leurs utilisateurs, cela n'est pas toujours à leur avantage. Outre les questions sur la protection des données, il existe toujours le danger que les données collectées se retrouvent sur Internet après un piratage ou une fuite. Bien que les microphones de Amazon Alexa puissent être éteints, il est plus pratique de les laisser allumés pour que l'assistant numérique puisse être activé à tout moment par la voix. Cependant, cela signifie aussi que des discussions privées pourraient être enregistrées. Les enregistrements ne sont pas analysés par l'appareil lui-même, mais par le cloud de Amazon. La société se réserve le droit d'enregistrer des enregistrements vocaux pour améliorer ses services - les cas où la police a recours à de tels enregistrements, par exemple en cas de meurtre, sont de plus en plus fréquents. Et si les discussions privées se retrouvent sur le cloud et fuitent ?
Les risques des données des bracelets de fitness et de santé quand elles tombent entre de mauvaises mains semblent évidents : Personne ne souhaite que des tierces personnes aient accès à son état de santé. De manière générale, la plupart des appareils IoT collectent des données qui en disent long sur leurs utilisateurs. A première vue, il n'est p.ex. peut-être pas évident ce que les données d'une ampoule intelligente disent sur une personne - mais à y regarder de près, on comprend qu'il est ainsi possible d'enregistrer les heures de présence de l'utilisateur et celles pendant lesquelles il dort. Si ces données tombent entre les mains de cambrioleurs, ceux-ci n'auront plus besoin d'observer pendant des semaines le comportement de leur victime et sauront en un coup d'œil quand passer à l'acte.
Outre le vol de données, il existe d'autres problèmes : parce que des millions de webcams IoT n'étaient pas suffisamment sécurisées, elles ont été piratées et utilisées comme botnet pour des attaques DDoS. Grâce à plusieurs millions de demandes, les hackeurs ont pu faire plier des réseaux informatiques étrangers. Sans oublier le danger du ransomware : si l'ordinateur est victime d'un tel malware de chantage, dans le pire des cas, "seules" les données personnelles sont perdues. En revanche, si le thermostat, la serrure de la maison ou les ampoules ne fonctionnent plus parce que des hackeurs ont mis la main dessus et demandent une rançon, cela peut avoir des conséquences néfastes.

Quelles sont les contremesures ?

Bien qu'il existe déjà un grand nombre de produits IoT, le développement n'est qu'à ses débuts. Les utilisateurs rencontrent notamment le problème qu'il n'existe que très peu de standards et que chaque fabricant mise sur son propre système. Les "talents" de Amazon Alexa pourraient représenter une première consolidation dans ce domaine : comme les applis, les appareils IoT ou autres services peuvent attribuer un "talent" à Alexa, qui permet d'intégrer le contrôle via l'appareil Amazon.

Le danger est grand chez les appareils les moins chers notamment, pour lesquels la sécurité n'a pas été prise en compte et une technique désuète et

peu sûre est utilisée. En effet, pour les utilisateurs sans connaissances techniques il n'est pas possible de savoir si leur webcam IoT a été victime d'une attaque DDoS. Pour éviter de tels dangers, seule une recherche détaillée avant l'acquisition peut aider, ainsi qu'une mise à jour régulière du logiciel.
En ce qui concerne l'utilisation d'appareils IoT, la priorité absolue doit être la minimisation des données. Les assistants numériques notamment, qui "écoutent" sans cesse, représentent un danger pour la vie privée. Cependant, le fardeau n'est pas à supporter par les utilisateurs, mais par les fabricants des appareils. Lors d'une conférence à l'Ile Maurice, deux documents ont été adoptés : Mauritius Resolution on Big Data et Mauritius Declaration on the Internet of Things. Les deux résolutions reconnaissent que l'IoT, en lien avec le Big Data, peut nous faciliter la vie, mais que les fabricants de ces appareils ont une grande responsabilité en raison des grands volumes de données qu'ils produisent et analysent.

Les points suivants ont été retenus quant à l'IoT :

- l'autodétermination est un droit important pour tous les personnes
- les données collectées par les appareils IoT devraient être reconnues comme des données personnelles et traitées comme telles
- les fabricants des appareils IoT devraient mettre au clair quelles données ils collectent et pour quelles fins, et combien de temps les données seront enregistrées
- la protection des données devrait être intégrée dans le processus de conception de ces appareils
- les données devraient, autant que possible, être analysées sur l'appareil - sinon une connexion cryptée pour la transmission devrait être utilisée
- les autorités chargées de la protection des données devraient surveiller de près le respect des lois correspondantes
- tous les acteurs du secteur IoT devraient discuter de manière constructive sur les implications de l'IoT et les conséquences à en tirer

Internet des objets offre, notamment en rapport avec le BIG DATA, de nombreuses possibilités intéressantes. Malheureusement, il existe au moins autant de dangers qui nous guettent. Il est donc important de bien s'informer avant un éventuel achat d'appareil et de rester attentif.

Sources :

- Wikipedia: Trojan Room coffee pot
- faz: Konzerne verbünden sich gegen Hacker
- Wikipedia: IPv6 adress
- An Internet of Things
- Wenn die Kuh per Funk den Landwirt holt
- 10 Real World Applications of Internet of Things (IoT) – Explained in Videos
- 15 Examples of Internet of Things Technology in Use Today
- Internet of Things to generate 400 zettabytes of data by 2018
- The role of big data analytics in Internet of Things
- Ten examples of IoT and big data working well together
- Big data and the Internet of Things: Two sides of the same coin?
- Data Protection Officials Adopt Internet of Things Declaration and Big Data Resolution

Pour toute question au sujet de l'arnaque en ligne ou sur l'utilisation d'Internet en général, contactez la BEE SECURE Helpline:

BEE SECURE HELPLINE CONSEIL
Tél: 8002 1234

Editeur: BEE SECURE · B.P. 707 · L-2017 Luxembourg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.lu www.bee-secure.lu

BEE SECURE powered by Service National de la Jeunesse · SECURITY MADE IN.LU · kanner jugend telefon
März 18
THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union Connecting Europe Facility