

Faut-il apprendre à se méfier des jouets connectés ?

Trop vulnérables aux attaques informatiques ou carrément « indiscrets », les jouets connectés pourraient sérieusement menacer la vie privée de nos enfants.

« Des risques qui parfois donnent à imaginer les pires scénarios »

Julie Frère estime que les coups de sonde opérés ne plaident pas en faveur des jouets connectés et de leur sécurité supposée.

Les jouets connectés représenteraient des risques en matière de respect de la vie privée. Qu'en est-il exactement ?

On a récemment diffusé trois communiqués sur le sujet, fruit d'une série de coups de sonde effectués à différents endroits et par différents organismes. On a d'abord relayé une enquête réalisée l'année passée par nos collègues norvégiens, qui montrait qu'il y avait un problème particulier avec un robot et une poupée. Prendre le contrôle de celle-ci avec un téléphone portable, communiquer par son entreprise avec l'enfant ou écouter ce qu'il passait dans son entourage direct étaient, vérifications faites, des choses extrêmement aisées. Au niveau de

montres connectées pour enfants, on a également relevé des problèmes. Il est possible d'en prendre le contrôle à distance et d'indiquer par exemple que l'enfant se trouve à un endroit où en réalité il ne se trouve plus. En outre qu'advient-il de toutes les données collectées par les montres ? On ne le sait guère. Enfin, sur des robots connectés, on a découvert que des données collectées et non indispensables au bon fonctionnement du jouet

étaient communiquées à des sociétés tierces. Avec en plus, dans un cas, la possibilité de prendre le contrôle du jouet à distance. Ce qui laisse imaginer les pires scénarios : éventuellement qu'un étranger prenne le contrôle du jouet et fasse ainsi venir l'enfant vers lui dans un parc lors d'un moment d'inattention. Qu'est-ce que tout cela pose comme constat ? Certes, on n'a pas pu analyser l'ensemble des jouets

sur le marché. Mais à chaque fois qu'il y a eu un coup de sonde, on a constaté des problèmes de sécurité ou de respect de la vie privée. Le tout alors que ces jouets sont destinés à des enfants, donc à un public vulnérable. Ce qui nécessite d'être intransigeant au niveau des exigences de vie privée et de sécurité. Très clairement, pour l'instant, nous ne recommandons pas aux parents d'acquiescer ce genre de jouets connectés.

Les fabricants ont-ils péché par manque de précautions ? Ou ont-ils parfois des intentions plus troubles en revendant par exemple les données qu'ils ont pu obtenir ?

Les intentions des fabricants peuvent être ce qu'elles sont, il n'en reste pas moins qu'ils doivent respecter les réglementations, notamment en matière de vie privée. Revendre des données n'est pas interdit mais il faut respecter les règles en matière de vie privée. Il faut

informer les personnes et le cas échéant obtenir leur consentement. Au niveau de la sécurité, c'est plus flou. En Allemagne, les autorités ont interdit certaines montres connectées en indiquant qu'elles constituaient des appareils d'espionnage illégaux et ont appelé à les détruire. En Belgique, on n'a pas encore assisté à ce genre de réactions. On se renvoie la balle. Du côté de la Commission de la vie privée, c'est si-

lence radio pour l'instant.

Imaginons que les fabricants n'aient que des intentions vertueuses, ne resterait-il pas malgré tout le risque de piratage de tous ces appareils connectés ?

Sur les robots que nous avons analysés, nous en avons tout de même pointé pour lesquels il était beaucoup plus difficile de prendre le contrôle de la connexion et donc de l'appareil. Il y a donc aujourd'hui

des technologies qui permettent d'assurer tout de même un certain niveau de sécurité.

Faut-il un durcissement des législations selon vous ?

Oui, ces objets connectés ne rentrent pas dans un cadre légal spécifique. Pour l'heure, on tente d'utiliser les outils juridiques existants. Mais on devra, je pense, en arriver à une législation plus adaptée. ■

**Propos recueillis par
MATHIEU COLINET**

Julie Frère

Julie Frère est licenciée en droit. Elle est porte-parole de Test-Achats. Comme d'autres associations de consommateurs, l'organisme a récemment alerté sur les risques que représentaient les jouets connectés.

« Beaucoup d'objets connectés n'ont pas la sécurité ad hoc »

Jo De Muynck a accepté de préciser les risques liés à l'utilisation de jouets connectés en avançant toutefois une limite à l'exercice : ces risques sont théoriques.

Des poupées qui enregistrent les conservations des enfants, des formulaires d'inscription très « indiscrets », quels sont exactement les risques liés aux jouets connectés ?

Il y a une grande diversité d'objets connectés et donc une grande diversité de risques à considérer au cas par cas. Toutefois, si l'on veut résumer, il y a deux grandes caté-

gories de risques : risques liés à la protection de la vie privée et risques liés au fait d'introduire un "device", c'est-à-dire un appareil mobile sur lequel on n'a pas le contrôle dans le réseau de la maison.

Ces jouets sont-ils de nouveaux espions avec éventuellement ce que cela suppose d'intentions troubles des fabricants ? Ou font-ils davantage leur maladie de jeunesse en ne répondant pas encore à toutes les exigences de sécurité ?

Il y a une forte croissance des

objets connectés. Ils se doivent d'être compétitifs, innovants, attractifs... Pour les vendre, les fabricants mettent essentiellement en avant le design, les fonctionnalités, le prix de leurs produits. Travailler à une cybersécurité pour ces objets demande pas mal d'efforts. Pour l'heure, beaucoup d'objets connectés n'ont pas les systèmes de sécurité ad hoc. Au niveau européen, on cherche à mettre en place un système de certification, mais ce n'est pas encore le cas. Au niveau du Centre pour la cybersécurité Belgique, nous

sommes prêts à prendre part aux initiatives internationales en la matière pour imposer des normes de sécurité minimales sur les chaînes de production.

Est-il possible de se prémunir de ces risques sans pour autant bannir les jouets connectés ?

Les jouets connectés envoient des données à caractère personnel vers des tiers et l'utilisateur n'a pas ou peu de contrôle sur l'utilisation et la protection de ces données.

La responsabilité de la protection revient donc entièrement au constructeur. Il est le seul à avoir le contrôle sur le fonctionnement du jouet et sur la destination des données. Néanmoins, on peut donner quelques conseils de base aux utilisateurs : utili-

ser seulement les objets connectés avec un wifi protégé, recourir à des mots de passe forts, éteindre les appareils en cas de non-utilisation, surveiller les enfants lorsqu'ils utilisent les jouets connectés...

On parle des risques liés aux jouets connectés. Qu'en est-il des objets connectés plus généralement ?

De plus en plus d'objets sont connectés tels que des réfrigérateurs, des réveils, des voitures, des machines à café... Appelés « Internet of things » ou « Smart devices », ce sont des appareils de la vie de tous les jours auxquels un ordinateur ou une connexion internet a été ajouté.

Potentiellement, tous ces objets peuvent représenter un

risque en matière de protection des données. Le 21 octobre 2016, si vous vous en souvenez, une attaque du type « Distributed Denial of service », c'est-à-dire qui vise à saturer un service de connexion pour le rendre inaccessible, s'est produite. Ce jour-là, Dyn, l'entreprise au cœur des perturbations, a rapporté que plus de 10 millions d'adresses IP étaient concernées. Les appareils infectés faisaient partie du réseau botnet Mirai, un réseau connu pour infecter des appareils vulnérables « Internet of things », comme des webcams, des télévisions, des magnétoscopes, etc. C'est ce qui a donné de l'ampleur à l'attaque. ■

**Propos recueillis par
MATHIEU COLINET**

**Jo
De Muynck**

Jo De Muynck est directeur
du CERT.be, la « cyber emergency team » fédérale.