Les dangers des jouets connectés | Denis JACOPINI

Les dangers des jouets connectés | Denis JACOPINI

La gamme Cloudpets de Spiral Toys a été piratée. Plus de 800000 comptes ont été piratés avec les informations qui y sont liées et plus de 2,2 millions de messages vocaux se retrouvent également sur la toile. Les peluches connectées de la marque permettait en effet aux parents et aux enfants de s'échanger des messages par le biais d'une application téléphonique, à travers l'ours en peluche.

Denis JACOPINI a été Interviewé par la revue Atlantico à ce sujet :

Atlantico : Une société d'ours en peluche connectés a été récemment piratée, les messages laissés par les parents à leurs enfants sont désormais hackable. Ce n'est pas la première fois que ce type de piratage arrive, pour protéger nos enfants, devrions-nous les éloigner de ce type de jouets connectés ?
Denis JACOPINI : En effet, au-delà du risque relatif à la protection des données personnelles des enfants et de leurs parents, la revue Que choisir avait déjà alerté les consommateurs en fin 2016 sur des risques inhérents au connexions non sécurisée de plusieurs jouets connectés.
Qui a tenu compte du résultat de cette étude pour revoir la liste des jouets qui seraient présents dans la hotte légendaire ?
La relation entre les enfants et les jouets va bien au-delà de la technologie et des risques qu'elle peut représente.
Les jouets bénéficie également de phénomènes de mode et l'engouement, sauf erreur, se fout bien de la qualité des produits et encore moins de leur sécurité.
Manque de connaissance, inconscience, crédulité ou trop de confiance de la part des parents ? Il est vrai qu'on peut facilement croire que si des jouets se trouvent sur nos rayons, c'est qu'ils ont forcément dû passer avec succès toute une batterie de tests rassurant pour le consommateur.
Pour la part des jouets à usage familial testés, même si les normes EN71 et EN62115 ont été récemment révisées pour répondre aux exigences de la nouvelle directive 2009/48/CE, les validations se reposeront sur des niveaux satisfaisants en terme de propriétés physiques et mécaniques, d'inflammabilité, de propriétés chimiques, électriques ou bien relatives à l'hygiène et à la radioactivité.
Vous l'aurez remarqué, aucun test n'est prévu pour répondre à des mesures ne serait-ce que préventive en terme de protection des données personnelles et encore moins en matière se sécurité numérique.
Alors finalement, pour répondre à votre question : « devrions-nous éloigner les enfants de ce type de jouets connectés ? »
A mon avis, en l'absence de normes protectrices existantes, la prudence devrait être de mise. Certes, il est impossible de se protéger de tout. Cependant, il serait à minima essentiel que les parents soient informés des risques existants et des conséquences possibles que pourraient provoquer des piratages par des personnes mal intentionnées pour prendre des mesures qu'ils jugent utiles.

Atlantico : Comment pouvons-nous restreindre la possibilité de piratage de données pour ce type d'objet ?
D.J. : La situation confortable serait que le consommateur soit vigilant pour ce qui concerne les mesures de sécurité couvertes par l'appareil et celles qui ne le sont pas. Malheureusement, ces gardes-fous ne sont qu'à l'état d'étude.
Sauf à vous retrouver dans un environnement ou le voisin le plus proche se trouve à plusieurs dizaines de mètres, être prudent dans l'usage de ces objets pourrait par exemple consister à :
– Si le jouet le permet, changer le mot de passe par défaut et mettre en place un mot de passe complexe pour accéder à sa configuration ;
– Si le jouet le permet, activer les connexions sécurisées par cryptage ;
– Si le jouet le permet, désactiver les connexions à partir d'une certaine heure ;
– N'utiliser les jouets connectés que dans des environnements protégés, en raison de la portée limitée des communications Bluetooth (par des distances suffisantes entre le jouet et des pirates éventuels) ;
– Pour les jouets utilisant le Wifi,
– Mettre en place des protections physiques contre les rayonnements électromagnétiques dans certaines directions ;
– Cacher les caméras si elles ne sont pas utilisées ;
– En fin d'utilisation du jouet, ne pas se satisfaire d'éteindre l'appareil qui ne sera peut-être seulement en veille, mais retirer les piles ou placer le jouet dans un espace protégé (fabriquez une cage de Faraday) ;
Enfin, compte tenu que le bon fonctionnement du jouet est lié à l'acceptation des conditions contractuelles d'utilisation des donnés personnelles ne respectent pas les règles européennes relative à la protection de ces données et de la vie privée car les fabricants sont généralement situés hors Europe, ne pas accepter ces conditions reviendrait à être privé de l'usage des fonctions du jouet.

Atlantico : Concrètement, les objets connectés sont une porte ouverte à notre intimité, quels sont les dangers liés à ce type d'objets ?
A défaut d'information de la part des fabricants et d'alerte de la part des médias, il serait, à mon avis, adapté que le consommateur reconsidère les objets numériques et particulièrement les objets connectés comme étant des équipements dont les fonctions et conséquences induites risquent de se retourner contre son utilisateur.
L'année dernière, l'association de consommateurs UFC-Que choisir a mis en garde les consommateurs sur le stockage des données. Elle a d'ailleurs saisi sur le sujet la Commission nationale de l'informatique et des libertés et la Direction générale de la concurrence, de la consommation et de la répression des fraudes.
En effet, tout ce que disent les enfants à la poupée testée est enregistré et mystérieusement stocké sur des serveurs à l'étranger et géré par la société Nuance Communications. L'Association européenne de défense des consommateurs a déclaré : « Tout ce que l'enfant raconte à sa poupée est transmis à l'entreprise, basée aux États-Unis, Nuance Communications, spécialisée dans la technologie de reconnaissance vocale ».
Quelles sont les conséquences d'un tel usage de nos données ?
L'objectif évident est le matraquage publicitaire des enfants, car certains jouets ont une certaine tendance à faire souvent allusion à l'univers de Disney ou à Nickelodeon par exemple.
Enfin, des tests ont montré qu'un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom Bluetooth par défaut du jouet connecté, permet très simplement de les identifier.
Plus grave encore… Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.
Que ça soit en en terme d'écoute et d'espionnage à distance de l'environnement de l'enfant et de celui des parents, ou en terme de prise de contrôle à distance de l'appareil risquant de terroriser ou pire, traumatiser l'enfant, la prudence doit d'abord rester de mise.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..
(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Jouet connecté : après un piratage, les données de 800000 familles fuitent sur le web*