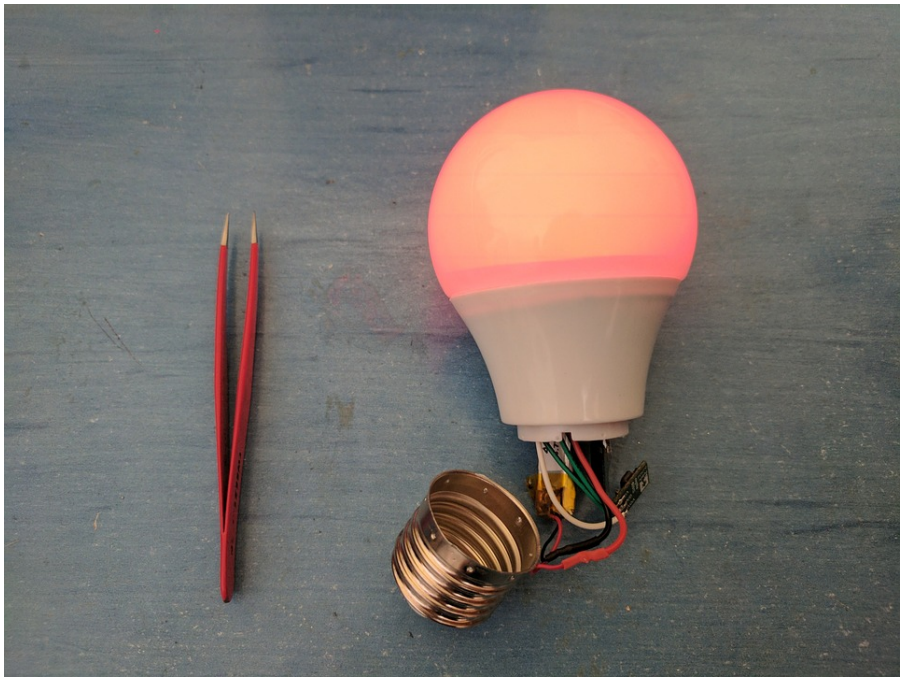
La problématique des objets connectés trop indiscrets



La problématique des objets connectés trop indiscrets

Brancher le baby phone, activer le thermostat, prendre sa tension ou sa température… Gestes loin d'être anodins dans l'internet des objets.

On a récemment évoqué dans les médias le danger potentiel d'un aspirateur automatique baptisé Roomba. Ses algorithmes et capteurs détectent les objets et obstacles, de manière à établir une cartographie des pièces où il est utilisé. Chez le fabricant, on précise que ces données servent à améliorer le matériel. Les détracteurs prétendent que les données récupérées sont vendues. Peu importe, la prudence s'impose avec les objets du quotidien connectés sur Internet.

Pas de budget pour la sécurité

Frigos, pacemakers, smartwatchs, babyphones et téléviseurs derniers cris peuvent désormais présenter un danger. Samsung conseille ainsi de désactiver la reconnaissance vocale sur ces Smart TV afin d'empêcher que vos conversations privées puissent être interceptées! Ces TV intelligentes disposent de deux microphones; un à l'intérieur du téléviseur, l'autre à l'intérieur de la télécommande afin d'interagir avec votre Smart TV à la voix. Un fournisseur de services tiers convertit vos commandes vocales interactives en texte et dans la mesure nécessaire pour vous fournir les fonctionnalités de reconnaissance vocale. Le fabricant insiste sur le fait qu'il utilise le cryptage standard de l'industrie pour sécuriser les données.

Multinationales ou start-up mettent aujourd'hui sur le marché des produits connectés où la sécurité pour protéger les données est reléguée au second plan pour des raisons de budget. Ces appareils disposent de petits processeurs capables de traiter un nombre d'instructions limité. Au point qu'aujourd'hui l'industrie récompense les personnes aidant à remonter des bugs de sécurité (sites, applications etc.) via les bug bounty qui mettent en contact ceux qui cherchent et trouvent les failles avec les développeurs de produits. Une stratégie préventive de sécurité qui en appelle d'autres…[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Réglement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS

: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle)

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 : *La problématique des objets connectés trop indiscrets – Toute l’actu 24h/24 sur Lavenir.net*