Publicado en Madrid el 25/05/2023

Los ‘Smart toys’ pueden espiar de forma ilícita en los hogares

Un informe realizado por la compañía de ciberseguridad S2 Grupo revela que el principal ciberpeligro de los juguetes inteligentes o 'smart toys' es que pueden espiar de forma ilícita los hogares, robar datos personales, credenciales de acceso, datos almacenados, imágenes y sonido, toma de control remoto del dispositivo, interceptación de las comunicaciones, ataques de denegación de servicio y elevaciones de privilegios o suplantación de identidad

Según ha indicado José Rosell, socio-director de S2 Grupo, durante la rueda de prensa que tuvo lugar para presentar el informe Investigación sobre juguetes inteligentes, hay que tener en cuenta que "estos ciberpeligros conllevan daños importantes contra la privacidad de los menores y los hogares. Debido a la naturaleza y a las limitaciones técnicas de este tipo de dispositivos, hemos detectado niveles muy bajos de seguridad en ellos y esto es especialmente grave porque la información confidencial que puede verse comprometida pertenece a menores de edad, uno de los colectivos más vulnerables".

Como se aclara en la investigación, los 'smart toys' están en pleno auge en Europa. Cada vez son más los niños que cuentan con al menos un juguete inteligente en casa y se espera que sus ventas aumenten hasta 2026 un 28%. Y este incremento se verá todavía más estimulado con las tecnologías 5G. Se estima que la cantidad de suscripciones de teléfonos inteligentes 5G alcance los 2.451 millones para 2025 en comparación con los 580 millones para fines de 2021.

"Los juguetes inteligentes están caracterizados por contener elementos electrónicos integrados para que puedan adaptarse a las propias actividades del usuario. De este modo, los juguetes inteligentes pueden procesar más información de una mayor variedad de sensores como, por ejemplo, micrófonos, reconocimiento de voz, cámaras, sensores de proximidad, transmisores de radio o bluetooth para establecer comunicaciones entre varias partes del juguete. El dispositivo está controlado por software y contiene elementos de inteligencia artificial, cuestión que implica la capacidad de aprender y procesar información del usuario", ha explicado Rafael Rosell, director comercial de S2 Grupo.

Por todo esto, expertos de la compañía han incidido en que los consumidores, especialmente los adultos, deben ser conscientes de los riesgos que estos juguetes pueden presentar. Además, han resaltado que las empresas jugueteras han de cumplir la normativa jurídica y técnica elaborada al respecto, con el fin de garantizar la protección de datos de los usuarios. Y han recomendado a las familias que el registro que realicen para usar estos juguetes sea con los datos mínimos imprescindibles y utilicen el derecho de libre acceso y destrucción a la información guardada por el smart toy.

Principales preocupaciones de las familias en relación a los smart toys

En el primer ‘Informe sobre la ciberseguridad de los smart toys', el equipo de S2 Grupo ha destacado que los juguetes inteligentes pueden aportar importantes beneficios a los niños en términos

de aprendizaje, entretenimiento, e incluso desarrollo socio-cognitivo. Por este motivo, los padres perciben la tecnología como una fuerza de progreso que puede tener una significativa capacidad para transformar y mejorar la vida de sus hijos, pero también les genera preocupación.

En este sentido, el 77% de los padres están preocupados por proteger la privacidad digital de sus familia, al 73% de los padres les preocupa que terceros recopilen datos personales sin su consentimiento, el 90% reconocen la importancia de proteger la identidad de sus hijos, la ubicación (88 %), los datos de salud (87 %), la edad (85 %), los registros escolares (85 %) y el historial de navegación (84 %)".

Respecto a qué tipo de acciones se deberían llevar a cabo en materia de seguridad dentro de la prevención parental se han extraído las siguientes conclusiones. El 86% de los padres piensa considera que es de alta relevancia mantener canales de comunicación activos y fluidos donde se pueda hablar abiertamente sobre la privacidad, la seguridad y la protección.

El 75% de los progenitores considera que una charla sobre seguridad y privacidad con sus hijos es tan importante como puede darse en el terreno de la sexualidad.

El 89 % de los progenitores considera que deben disponer de herramientas de control que les permita desempeñar un rol de seguridad con sus hijos.

El 91% de los padres quieren que las aplicaciones sean revisadas por expertos en cuanto a privacidad y seguridad antes de que estén disponibles para su descarga.

Recomendaciones de uso seguro de juguetes inteligentes
Desde S2 Grupo se han señalado que algunas recomendaciones para el uso seguro de los smart toys son:

Supervisar la actividad de los más pequeños con este tipo de dispositivos.
Comprobar si hay chat en ese juguete y si requiere la ubicación.
Se recomienda utilizar aquéllos que disponen de control de seguridad para los padres.
Comprobar que el juguete cuenta con un componente físico o digital de acceso a la red y que son los padres los que dan acceso al mismo.
Leer con detenimiento la política de privacidad y seguridad de los juguetes digitales.
Apagar siempre el juguete cuando no se esté utilizando.

Por último, en el evento celebrado por S2 Grupo se han analizado algunas de las polémicas en ciberseguridad en juguetes inteligentes desde 2015 y se ha realizado una demostración práctica del hackeo de un juguete inteligente.

Datos de contacto:
Luis Núñez Canal
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Juegos Ciberseguridad Consumo Dispositivos móviles