

Cuando la pantalla observa: la vigilancia silenciosa de los Smart TV

Durante años pensamos el espionaje como algo lejano: agencias de inteligencia, hackers sofisticados o ataques a grandes empresas. Hoy, sin embargo, una parte relevante de la vigilancia digital ocurre en un lugar mucho más cotidiano y despreocupado: el living de la casa. Y el protagonista no es un micrófono oculto, sino el televisor inteligente colgado en la pared.

Los números ayudan a dimensionar el fenómeno. A nivel global, más de mil millones de hogares ya tienen al menos un Smart TV conectado a internet, y en Chile el televisor sigue siendo la principal pantalla del hogar. Más del 90% de las personas consume contenido audiovisual desde un televisor, y en los hogares con televisión conectada, el 95% utiliza directamente un Smart TV, no un dispositivo externo. En la práctica, el Smart TV se ha convertido en el computador más masivo del hogar, siempre encendido, siempre conectado y casi nunca cuestionado.

Pero este televisor ya no es solo una pantalla. Es un dispositivo con sistema operativo, tiendas de aplicaciones, sensores y, en muchos modelos, micrófonos activos para comandos de voz. Desde la perspectiva de la ciberseguridad, esto lo transforma en una plataforma ideal para la recolección de datos. No necesariamente para “escuchar” conversaciones completas como en una película, sino para algo más silencioso y efectivo: observar comportamientos.

Diversas investigaciones han demostrado que los Smart TV utilizan tecnologías de reconocimiento automático de contenido que permiten identificar todo lo que aparece en la pantalla, incluso cuando el televisor se usa solo como monitor conectado a una consola o a un notebook. Algunos modelos capturan imágenes o fragmentos de audio de forma periódica para reconocer programas, películas o videojuegos. Esa información se envía a servidores externos y se cruza con horarios, aplicaciones utilizadas, dirección IP y otros identificadores técnicos.

¿El resultado? Perfiles sorprendentemente precisos. A qué hora se prende el televisor, cuánto tiempo permanece encendido, qué tipo de contenido se consume, si hay niños en la casa, si se ven noticias, deportes o plataformas de streaming, e incluso cuándo el hogar suele estar vacío. No se espía una conversación aislada: se perfila una rutina completa.

En este escenario, surge una pregunta incómoda que rara vez nos hacemos: ¿cuándo fue la última vez que desconfiamos de nuestro televisor? Nos enseñaron a sospechar de correos extraños, de llamadas desconocidas o de enlaces dudosos, pero casi nunca de los objetos que conviven silenciosa-

mente con nosotros todos los días. El Smart TV, que alguna vez fue símbolo de modernidad y comodidad, se ha convertido, sin que lo notemos, en una especie de “ventana inversa”: mientras nosotros miramos hacia afuera para entretenernos, otros miran hacia adentro para entendernos. Y en ese cruce de hábitos, datos y algoritmos, la intimidad del hogar empieza a depender menos de cortinas cerradas y más de configuraciones que casi nadie revisa.

Esta información, tomada de forma individual, puede parecer trivial. Pero agregada a gran escala, permite construir mapas de comportamiento social, cultural y económico de millones de hogares. Y lo más inquietante es que no requiere vulnerar sistemas ni “hackear” dispositivos: basta con aprovechar permisos aceptados durante la configuración inicial del televisor o al instalar una aplicación.

El problema es que este tipo de vigilancia ocurre de manera silenciosa y normalizada. Los televisores recopilan datos incluso cuando se usan como simples pantallas externas, y muchas aplicaciones envían información a terceros sin que el usuario tenga claridad real sobre qué se recopila, con quién se comparte o por cuánto tiempo se almacena. El límite entre personalización, marketing agresivo y vigilancia se vuelve cada vez más difuso.

La buena noticia es que no se trata de una situación inevitable. Existen medidas simples que reducen significativamente la exposición: desactivar el reconocimiento automático de contenido, limitar o apagar el uso de micrófonos cuando no se utilizan, revisar qué aplicaciones están instaladas, mantener el sistema del televisor actualizado y evitar apps de origen dudoso. No eliminan el riesgo por completo, pero devuelven parte del control al usuario.

El televisor seguirá evolucionando, y con él, el ecosistema digital que habita nuestro hogar. Pero eso no significa que estemos condenados a renunciar a la privacidad. Por el contrario, hoy tenemos más herramientas que nunca para comprender, ajustar y decidir sobre nuestros propios datos. Recuperar el control es un acto de alfabetización digital: informarnos, preguntar, revisar y enseñar a otros a hacerlo. Porque en la era de los dispositivos inteligentes, el usuario también debe volverse más inteligente.



Edgardo Fuentes Cáceres – Director Ingeniería en Ciberseguridad UNAB

.....