Publicado en Madrid el 21/11/2019

El "humano conectado" el verdadero reto de la ciberseguridad

De toda la información personal que hay disponible sobre una persona en Internet, la más sensible de todas es la que está relacionada con su salud. Sin embargo, el auge de las tecnologías 'wearables' y de las apps sobre salud está haciendo que cada día se suban a 'la nube' miles de datos críticos en lo que respecta a la ciberseguridad

Para entender los riesgos que hay en los 'wearables, primero hay que que ser conscientes de lo que son. Al hablar de este tipo de tecnología, a la mayoría de la gente se le viene a la cabeza los relojes y pulseras inteligentes, pero recientemente se han puesto de moda las aplicaciones para saber si un alimento es sano o no; unas apps que piden al usuario información personal relacionada con su salud (colesterol, intolerancias, alergias, índice de masa corporal o enfermedades crónicas).

Además de ello, en breve, estarán a la orden del día las 'prendas inteligentes'. Aunque el mercado ya cuenta con camisetas, como las de Ralph Lauren, que monitorizan la actividad física para deportistas, los 'dispositivos vestibles' llegarán en breve al usuario de a pie, y también al sector profesional. Sin ir más lejos, la firma china Xiaomi, ya cuenta en su catálogo con varias prendas inteligentes a un precio accesible.

Teniendo en cuenta este contexto de monitorización constante, hay que tener en cuenta que si esos datos que cada persona comparte con una app o wearable conectado a la nube caen en malas manos, grupos organizados de ciberdelincuentes podrían saber cuál es su índice de colesterol, cuántas horas duermen al día, por dónde salen a correr, etc. Pero, también tendrían conocimiento sobre datos tan críticos como las alergias o intolerancias, los problemas cardíacos o si los órganos podrían ser compatibles con las de alguien que los requiera.

Usos profesionales de los weareables

Varias compañías ya han desarrollado y utilizan en sus 'plantas de trabajo inteligentes' dispositivos para optimizar las labores del nuevo 'empleado conectado': cascos y botas e incluso guantes y chalecos inteligentes, que dan instrucciones personalizadas a cada profesional para que sean más productivo o para evitarles daños en la espalda si tienen que levantar peso o cavar una zanja.

Sin ir más lejos, ya existen gafas inteligentes, como las de la compañía británica SEE, que detectan si un conductor está demasiado cansado como para seguir su ruta y le avisan de que debería descansar un rato para no poner en peligro su vida o la del resto de personas que circulan por la carretera.

"La ciberseguridad en todo este tipo de dispositivos debería ser una de las mayores preocupaciones, tanto de los fabricantes como de las empresas que los utilizan para sus empleados. La infinidad de riesgos en la integridad de los profesionales de una empresa, así como los datos personales que generan los wearables es de tal sensibilidad, que debería generarse un consenso en todo el tejido empresarial y estatal para velar por la ciberseguridad de estos dispositivos, advierte Hervé Lambert,

Global Consumer Operations Manager de Panda Security.

La importancia de los datos médicos
Y, por supuesto, no hay que olvidar los datos médicos. “El principal problema es que los ciudadanos de a pie tienden a pensar que a nadie le puede interesar tener esa información, porque ‘no son nadie'. Pero, pensar así es un grave error”, afirma Hervé Lambert. Sin ir más lejos, este mismo año se filtraron los datos personales del primer ministro de Singapur en Internet, causando una crisis que no fue resuelta hasta que el gobierno recuperó el control de la información.

Otro buen ejemplo de ello es el ataque que recibió en 2015 la compañía estadounidense UCLA Health, en el que un grupo de ciberdelincuentes accedió a los datos personales y médicos de 4,5 millones de pacientes porque sus servidores no estaban correctamente cifrados.

Estos casos sirven para poner en perspectiva el verdadero riesgo que hay en estas apps y dispositivos: alguien podría atacar sus servidores y filtrar a la Dark Web la información que contienen, haciéndose con millones de de datos críticos sobre salud. Así, antes de descargar una de estas aplicaciones o de comprar uno de estos dispositivos, es importante comprobar qué uso hacen de la información, cómo se almacena y dónde están sus servidores físicamente.

Lo ideal sería que aunque alguien accediese a esa información, no pueda relacionarla con el usuario. Para eso, es recomendable no dar nunca el nombre completo y usar una cuenta de correo electrónico alternativa. Asimismo, hay que contar con medidas de seguridad en el móvil para que los datos no puedan ser interceptados cuando viajan hasta el servidor en el que se aloja la app. En este sentido, es recomendable usar VPNS y apps de seguridad que auditen la navegación.

“Pero sobre todo, hay que tener sentido común. Al igual que uno no pone en la vida offline sus datos personales al alcance de cualquiera, tampoco debe descuidarlos en el mundo digital”, advierte Hervé Lambert.

En este sentido, hay que recordar que no hay que conectarse nunca a una wifi pública cuando se usen estas apps. Con lo que habría que decirle al móvil que estas apps nunca estén activas si no se están usando.

Y, por supuesto, “hay que contar con métodos para eliminar toda la información que hay en el móvil en caso de que sea robada o se pierda”, sentencia el directivo de Panda Security.

Datos de contacto:
Luis Núñez
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Moda Sociedad Digital Software Seguridad Aplicaciones móviles