La (in)seguridad en la palma de la mano

Los riesgos de la móvil-dependencia actual

Centralizar funciones e información en un dispositivo móvil puede ser de gran comodidad, aunque no siempre esto se traduce en seguridad. Robo del dispositivo y sus datos almacenados son un riesgo permanente para el usuario, riesgo muchas veces desconocido o no valorado.

Claudio Javaloyas
SEdeAP Argentina
sedeap@yahoo.com.ar

Así como la inteligencia artificial (IA) evoluciona en el universo del Internet de las Cosas (IdC) y las apps se extienden, actualmente el mayor desafío planteado es el reconocimiento del usuario para ejecutar sus preferencias, como si de un fiel y atento mayordomo y guardaespaldas se tratara.

Esta adicción que las sociedades actuales están sufriendo, la móvil-dependencia, es cada vez más profunda y se arraiga rápidamente creando falsas expectativas, las que pueden resultar muy peligrosas. La creencia de que un dispositivo móvil (ya sea un smartphone, reloj o tablet) puede brindarnos "seguridad" es grave si se confía ciegamente en ello.

Es importante tener el dispositivo móvil permanentemente bloqueado, protegido y encriptado, porque de perderlo o ser robado, los delincuentes podrían tener amplia ventaja y, además, el usuario mismo queda "desvalido" sin su acceso durante ese período.

Actualmente podemos acceder con el dispositivo móvil a las videocámaras, abrir puertas, desactivar alarmas, abrir la cochera, encender el auto, activar la domótica y operar en un home banking, además de los recientes DNI digital, registro de conducir, seguro automotor, billetera virtual, archivos y documentos personales con información sensible e importante.

Por si fuera poco, el móvil tiene almacenados los datos de contacto de familiares, amigos y clientes.

Confiar y depender demasiado del dispositivo móvil puede ser un problema de seguridad personal importante, ya que es el método predilecto de la mayoría de las personas para interactuar con la IdC e incluso se utiliza como botón antipánico, para pedir ayuda y ser geolocalizado a través de su GPS, pero es demasiado frágil, debe ser recargado constantemente y es uno de los objetivos preferidos por ladrones y asaltantes, junto con el dinero y las joyas.

CONCEPTO DE SEGURIDAD

La idea de que estos dispositivos móviles puedan proveernos "seguridad" es irreal, ya que la seguridad física debe protegerse con elementos físicos que impidan o compliquen mucho el asalto, robo o secuestro y no con vigilancia virtual, haciendo solamente llamadas y avisos ruidosos, ya que sería como protegerse de un león hambriento gol-

peando una olla para espantarlo.

El dispositivo móvil es útil, sin embargo, como complemento de una seguridad integral, para conseguir alguna ayuda adicional como de la policía o bomberos, y para el confort diario.

Debe uno mantener siempre una copia global de su dispositivo móvil en un formato seguro: sus datos, contactos, apps, fotos y videos deben estar disponibles por si se pierde, lo roban o se arruina y debemos adquirir otro nuevo, preparándolo para nuestro uso. Asimismo, debemos asegurarnos que el anterior dispositivo móvil no pueda ser usado en nuestra contra con autobloqueo, contraseñas y swipes complejos, además de la posibilidad del borrado y anulación remota si es robado.

EL CAMINO DE LA IDC

Sin dudas Internet de las Cosas seguirá evolucionando muy unida a la inteligencia artificial, logrando potenciarse al permitir mayor interacción con el usuario, de manera más natural e intuitiva con la interface de voz, que parece ser la más aceptada y actualmente de mayor desarrollo.

Las comisiones de seguridad de Europa y Norteamérica están proponiendo un estándar para que los fabricantes de dispositivos móviles e IdC provean de mayor eficiencia y seguridad en los datos y comunicaciones máquina a máquina (machine to machine o m2m, según su denominación en inglés) y protección adicional para los datos y configuraciones de los usuarios, para que no sean pirateados ni copiados por otros dispositivos ni puedan conectarse simultáneamente, evitando

"clones y gemelos" que puedan vulnerar la seguridad de la vida digital de los usuarios.

Hace unos meses, una marca líder de vehículos se vio comprometida en su app de comandos para control de sus productos, ya que la tecnología de proximidad utilizada podía ser canalizada en tiempo real por un dispositivo móvil próximo al usuario víctima y enviarla a otro móvil próximo al vehículo, que actuaba como si estuviera en presencia del real dueño.

Esta operatoria permitía al grupo de ladrones abrir y arrancar el auto, sustraer partes o introducirse alguien dentro y secuestrar al usuario a su regreso. Además, podía copiar los demás códigos de seguridad, de la cochera y otros accesos automatizados o domotizados con lo que los ladrones luego podían robar en los domicilios de las víctimas, ingresando por las rejas y portones sin problemas.

También con este método accedían al GPS del vehículo y del dispositivo móvil, obteniendo recorridos y geoposicionamientos anteriores y posteriores al clonado, ya que el GPS podía ser interrogado con la app de VTrack y seguirlo o esperarlo en una emboscada.

Algo similar sucedió con los Smart TV de una marca líder, en los cuales los delincuentes podían conectarse a su red WiFi, habilitar la cámara de videochat, y ver todo su historial de videos y películas en las redes así como la agenda, los recordatorios y hasta revisar algunas redes sociales de la víctima. De este modo luego podían intentar chantajes y aprietes a cambio de no divulgar los videos y datos obtenidos.

Tener la TV, la heladera y el auto conectado online no siempre es una buena idea. Mucho menos si no se tienen en claro sus peligros y beneficios. Más si además llevamos en el bolsillo o en la palma de la mano la llave y control remoto de todo y puede ser tomado por ladrones, no sólo por su valor como reventa sino por el mundo digital de información y datos personales allí acumulados. ■

Más información de los módulos y sus especificaciones en:
www.sedeap.com.ar