BYOD, la tendencia para trabajar con dispositivos personales y con seguridad

El enorme desarrollo que han experimentado los dispositivos electrónicos e informáticos de uso doméstico durante los últimos años y, más recientemente, la influencia de la pandemia, han extendido en el terreno empresarial el fenómeno BYOD (acrónimo de Bring Your Own Device). Hablamos de un hábito que consiste en que las personas empleadas por una empresa opten por utilizar sus propios ordenadores portátiles, smartphones y tabletas para conectarse a la red y a otros recursos corporativos en el ámbito del trabajo, en lugar de usar las herramientas que ofrece la propia compañía.

Si tu empresa está pensando en establecer políticas de BYOD o se ha detectado esta práctica y se desea regularizar la situación, protegiendo así la información sensible de la misma, la información que te aportamos a continuación puede ayudarte a hacer balance del riesgo-beneficio y seguir algunas recomendaciones.

Ventajas e inconvenientes del BYOD

En el lado positivo de la balanza, el hecho de utilizar equipos personales para uso profesional aporta:

- **Reducir** de forma considerable **la inversión en hardware y software** por parte de las organizaciones, ya que es la propia plantilla quien aporta, por ejemplo, su teléfono móvil.
- Mayor **flexibilidad y comodidad** por parte de la plantilla de trabajo. Continuando con el ejemplo anterior, pensemos en la ventaja de llevar un único teléfono móvil en lugar de dos.
- Incremento de **productividad** y eficiencia, por la posibilidad de atender cualquier asunto importante, en cualquier momento y lugar.
- **Facilita** considerablemente **el teletrabajo**, una modalidad que ha crecido de forma notable durante la pandemia.

Por otro lado, sin perder de vista que:

- **Se añade el riesgo corporativo al personal** en el hecho de que la información almacenada en los dispositivos, pueda extraviarse, ser robada o ser utilizada con fines maliciosos.
- Se abre una **nueva puerta de entrada al malware** a través de estos dispositivos, ya que en el momento en que el usuario se conecte con ese dispositivo personal a la red corporativa podría expandir dicha intrusión por toda la red de la empresa.
- Los **aspectos legales** derivados del uso de una tecnología personal o privada en el ámbito laboral en cuanto a confidencialidad de la información, responsabilidades, uso de licencias, etc. La AEPD ofrece una guía con algunas recomendaciones para proteger los equipos durante el teletrabajo.

Sin duda, unos riesgos que pasan por protocolizar, controlar dichos dispositivos e identificar los distintos puntos débiles que pueden generar en el conjunto de la infraestructura de ciberseguridad de la empresa. Así como por la difusión y el fomento de unas buenas prácticas para su uso. Algunas herramientas específicas como las de MDM (Mobile Device Management) pueden ayudar.

Mobile Device Management, una herramienta de gestión

Las herramientas de Mobile Device Management (MDM) ayudan a controlar de forma remota y a gestionar los dispositivos móviles que se conectan a su red y utilizan sus recursos corporativos. Permite administrar y realizar un seguimiento de las acciones efectuadas a través de los smartphones, tablets u ordenadores portátiles corporativos, desde los permisos para la instalación de aplicaciones hasta la geolocalización de los dispositivos y su protección en caso de pérdida o robo.

Su funcionamiento es sencillo, solo es necesario instalar la aplicación en el dispositivo que se quiere gestionar. A partir de ese momento el MDM crea una base de datos accesible para el administrador que puede detectar malware o cualquier tipo de incidencia; supervisar su actividad; configurarlo o bloquearlo remotamente, y generar informes de gestión. Esta herramienta puede instalarse en los dispositivos personales de los usuarios y diferenciar entre los datos personales y corporativos, tal y como se explica en el Informe de Amenazas CCN-CERT IA-21/13.

Recomendaciones de ciberseguridad para minimizar los riesgos

A pesar de que hoy en día es imposible garantizar la seguridad de nuestros equipos al 100%, sí podemos concienciar a la plantilla a través de una serie de recomendaciones para minimizar riesgos:

- Descarga, instala y actualiza únicamente las **aplicaciones** que estén permitidas en las políticas de seguridad de la empresa. Es importante que a la hora de descargarlas utilices markets oficiales. Además, es importante leer bien sus condiciones de uso para controlar los permisos de acceso sobre los dispositivos.
- Asegúrate que los **servicios de almacenamiento de datos** que emplees estén autorizados por la empresa mediante comunicaciones cifradas.
- A pesar de que la realización de **copias de seguridad** no nos protege de los ataques, sí que nos ayuda a recuperar rápidamente la información importante en el caso de que el dispositivo sea atacado y se vuelva inaccesible.
- **Cifra todos los dispositivos** para que el acceso no autorizado a la información sea más complicado para los ciberatacantes.
- En el caso de pérdida o robo de tus dispositivos, la herramienta de **localización remota** puede ser de gran ayuda ya que tiene varias funciones, entre ellas la localización de terminales, el bloqueo remoto del terminal, el borrado remoto de datos o el seguimiento de la actividad del dispositivo para vigilar las aplicaciones que se ejecutan.
- Utiliza siempre que sea posible comunicaciones seguras como una **Red Privada Virtual** (VPN) y evita conectar tu equipo a redes públicas.

Además de estas recomendaciones, es imprescindible que tanto las empresas como las personas que las integran conozcan de primera mano las amenazas y vulnerabilidades derivadas del uso de internet, y se conciencien de la necesidad de usar la tecnología de forma segura, especialmente en entornos BYOD.

La ciberseguridad presenta retos constantes a los que las empresas y las agrupaciones empresariales deben hacer frente cada día. Desde el BCSC queremos ayudar a las empresas a cubrir y dar respuesta a sus necesidades en ciberseguridad, y para alcanzar este objetivo, ofrecemos jornadas de sensibilización y formación en materia de ciberseguridad para las personas, desarrolladores, empresas, industria, Pymes y directivos de empresas.

Este fenómeno del que hemos estado hablando, está incluido en el Calendario de concienciación sobre Ciberseguridad de la European Ciber Security Organisation (ECSO) del mes de septiembre, una iniciativa que pretende aportar información útil sobre diferentes aspectos relacionados con la ciberseguridad.