Cómo usar el USB en la empresa para evitar ciberataques

Valladolid - El uso del pendrive en la empresa sigue siendo una solución rápida y eficaz para transportar información, pero también representa uno de los mayores riesgos de ciberseguridad para las pymes españolas.

De hecho, según el informe “Ciberpreparación de las empresas españolas 2024” de Hiscox, el 53% de las pequeñas y medianas empresas ha sufrido al menos un incidente de ciberseguridad en el último año, y los dispositivos USB siguen figurando entre los vectores de ataque más habituales.

Para ayudar a proteger la información de las empresas, la tecnológica Cosmomedia ha desarrollado un Manual de buenas prácticas en el uso de dispositivos USB, en el que aborda una serie de claves indispensables que toda pyme debe contemplar.

El USB, un riesgo real para la seguridad de la empresa

El uso inadecuado de dispositivos USB en la empresa puede suponer riesgos significativos como la propagación de malware, la pérdida o robo de datos sensibles y el acceso no autorizado a información confidencial.

Además, estos dispositivos pueden facilitar la alteración de configuraciones del sistema o la copia rápida y discreta de datos sin dejar apenas rastro, lo que incrementa el peligro de filtraciones y daños a la infraestructura tecnológica.

Claves en el uso del dispositivo USB para proteger la información en la pyme

Los principales normas o recomendaciones en el uso de dispositivos USB que establece la tecnológica en su manual de buenas prácticas, para que las empresas puedan minimizar los riesgos son:

Solo dispositivos USB autorizados y registrados
Todos los dispositivos USB utilizados en la empresa deben ser propiedad de la organización o estar expresamente autorizados por el departamento de IT. Cada dispositivo debe estar inventariado con datos como número de serie, marca, modelo, responsable y fecha de registro

Prohibido el uso de dispositivos personales
El uso de pendrives personales en equipos corporativos debe evitarse o prohibirse. En casos excepcionales, debe solicitarse autorización formal y realizar una revisión técnica previa

Revisión antivirus obligatoria
Antes del primer uso y de forma periódica, los dispositivos USB deben ser escaneados con un antivirus actualizado. Si se detecta malware, el dispositivo debe ser bloqueado y aislado de inmediato

Cifrado de datos
Todo USB que almacena información sensible debe estar cifrado. Herramientas como BitLocker (Windows) o VeraCrypt permiten proteger los datos y evitar que sean legibles en caso de pérdida o robo

Uso asignado y control de préstamos
Cada dispositivo debe tener un responsable asignado. Si es necesario compartirlo, debe registrarse el préstamo en el sistema de IT, asegurando la trazabilidad del dispositivo en todo momento

Evitar el uso compartido y la ejecución de software
Los dispositivos deben ser de uso individual. Si se necesita compartir información, es preferible utilizar canales corporativos como almacenamiento en red o nube empresarial. Además, está prohibido ejecutar aplicaciones o instaladores directamente desde el USB

Protección física y etiquetado
El pendrive debe guardarse en un lugar seguro, protegido de humedad, polvo o temperaturas extremas, y estar claramente etiquetado con el nombre del responsable, departamento y número de inventario

No dejar el USB conectado sin supervisión
Nunca se debe dejar un dispositivo USB conectado a un equipo sin vigilancia, especialmente en zonas comunes o de acceso libre

Copias de seguridad a mayores que el USB
No almacenar la única copia de un archivo importante en un USB. Toda información relevante debe tener una copia de respaldo en servidores internos, almacenamiento en la nube o sistemas de backup autorizados

Expulsión segura del dispositivo USB
Siempre se debe expulsar el dispositivo de forma segura antes de retirarlo físicamente del puerto USB, para evitar la corrupción de datos y posibles daños al dispositivo o al sistema operativo

Los especialistas de ciberseguridad de Cosmomedia también recomiendan establecer un **procedimiento formal de autorización para el uso de dispositivos USB**, que incluya una solicitud formal por parte del empleado, detallando el uso y justificando la necesidad, una

evaluación técnica inicial para verificar si existen alternativas más seguras de envío y traspaso de datos. Este protocolo debería también contemplar el análisis del dispositivo y su registro en un inventario.

La responsabilidad en el uso de dispositivos USB está tanto en los usuarios como en la propia empresa, que debe establecer, vigilar y hacer cumplir las normas. En ese sentido, la adopción de estas buenas prácticas no sólo puede proteger la información corporativa, sino que también refuerza la confianza de clientes y proveedores.

En un contexto donde el 95% de las brechas de seguridad en pymes españolas tiene su origen en errores humanos o malas prácticas (fuente: INCIBE), la prevención y la concienciación se convierten en la mejor defensa frente a las ciberamenazas.

El Manual de buenas prácticas en el uso de dispositivos USB aborda de manera más detallada, los mejores protocolos de trabajo para que las pymes puedan reforzar su ciberseguridad y proteger sus datos frente a este tipo de amenazas silenciosas, escondidas muchas veces dentro de un aparente inofensivo pendrive.

Informe Ciberpreparación de las empresas españolas 2024
Manual: https://www.cosmomedia.es/blog/ciberseguridad/la-ciberseguridad-de-tu-empresa-y-el-uso-del-usb-protege-tus-datos-con-nuestro-manual-esencial?utm_source=prensa&utm_medium=organic&utm_campaign=ndp
Imagen generada por IA

Contacto de prensa:
Silvia Fernández
Teléfono: 983 666 555
comunicacion@cosmomedia.es