El desafío de la seguridad en los dispositivos de almacenamiento

En la era digital, la protección de la información es una prioridad para individuos y organizaciones. Los dispositivos de almacenamiento, , son esenciales para el resguardo de datos, pero también representan una de las principales vulnerabilidades en materia de seguridad de estos. ¿Estamos realmente preparados para garantizar su seguridad?

Uno de los principales riesgos es el acceso no autorizado a la información. Dispositivos de almacenamiento sin cifrado pueden ser fácilmente sustraídos o comprometidos, exponiendo datos sensibles. La solución más evidente es la implementación de cifrado robusto, pero sorprendentemente, muchas empresas aún no lo adoptan de manera generalizada.

Otro problema clave es la proliferación de dispositivos extraíbles. Si bien son prácticos, estos dispositivos pueden ser una puerta de entrada para malware y robo de información. Las organizaciones deben establecer controles estrictos sobre su uso, incluyendo restricciones de acceso y monitoreo continuo.

El almacenamiento en la nube también plantea interrogantes. A pesar de que los proveedores ofrecen medidas de seguridad avanzadas, los riesgos persisten, especialmente si los usuarios no adoptan buenas prácticas como la autenticación multifactor y la gestión adecuada de permisos.

La eliminación segura de los datos es un aspecto muchas veces ignorado. Recuperar información de un disco duro formateado es más fácil de lo que se cree, lo que hace indispensable la aplicación de técnicas de borrado seguro o destrucción física en casos críticos.

La seguridad de los dispositivos de almacenamiento no es solo una cuestión técnica, sino también de cultura organizacional y personal. Es imperativo que individuos y empresas adopten estrategias efectivas para proteger la información, entendiendo que la prevención siempre será la mejor defensa en el mundo digital.

Desde el punto de vista del Esquema Nacional de Seguridad (ENS), la mejor manera de gestionar los dispositivos de almacenamiento es adoptando un enfoque integral que combine medidas técnicas, organizativas y procedimentales. Este enfoque debe estar alineado con los niveles de seguridad establecidos (Básico, Medio y Alto) y contemplar los siguientes aspectos clave:

1. **Clasificación y Evaluación de la Información**

   - **Identificación y Clasificación:** Antes de gestionar cualquier dispositivo, es esencial clasificar la información almacenada en función de su sensibilidad. Esto permite definir el nivel de protección requerido y aplicar las medidas correspondientes.

2. Control de Acceso y Autenticación

- **Acceso Restringido:** Solo el personal autorizado debe tener acceso a los dispositivos de almacenamiento. Se deben implementar mecanismos de autenticación robustos que eviten accesos no autorizados tanto en el ámbito físico como en el lógico.

3. Cifrado de Datos

- **Protección en Reposo y en Tránsito:** Es imprescindible cifrar los datos almacenados utilizando algoritmos aprobados por el Centro Criptológico Nacional (CCN). El cifrado protege la confidencialidad de la información, incluso en caso de pérdida o robo del dispositivo.

4. Protección Física y Lógica

- **Medidas Físicas:** Los dispositivos deben ubicarse en entornos controlados y seguros, con acceso restringido a personal autorizado.
- **Medidas Lógicas:** Además del cifrado, es recomendable implementar firewalls, sistemas de detección de intrusiones y otras medidas de seguridad que dificulten el acceso no autorizado desde el ámbito digital.

5. Registro, Auditoría y Monitorización

- **Seguimiento de Accesos:** Se deben establecer registros de auditoría que documenten quién accede a los dispositivos y qué operaciones se realizan. Esta monitorización continua es clave para detectar y responder a posibles incidentes de seguridad.

6. Gestión de Dispositivos Extraíbles

- **Control Estricto:** Dado que los dispositivos extraíbles (como USB o discos duros portátiles) pueden representar una vulnerabilidad, es fundamental restringir su uso a través de políticas claras y herramientas de control que impidan la conexión de dispositivos no autorizados.

7. Procedimientos de Eliminación Segura

- **Borrado Irreversible:** Cuando un dispositivo de almacenamiento se retira de servicio o se desecha, deben aplicarse métodos de eliminación segura (como la destrucción física) para garantizar que la información no pueda ser recuperada.

En función de la categorización de los datos, y siguiendo con lo que dictamina el ENS, así como el tipo de organización tendremos las siguientes medidas técnicas y organizativas:

Medidas Técnicas

Cifrado de la Información

- **Nivel Básico:**

  Utilizar cifrado para datos sensibles en dispositivos externos, aunque de forma no obligatoria para toda la información.

- **Nivel Medio:**

  Implementar cifrado obligatorio en reposo y, cuando sea posible, también en tránsito. Se deben utilizar algoritmos aprobados por el Centro Criptológico Nacional (CCN).

- **Nivel Alto:**

  Requerir el cifrado de todos los datos almacenados en dispositivos externos con algoritmos robustos y certificados. Además, se puede exigir el uso de módulos criptográficos hardware (HSM) para operaciones críticas.

Monitorización y Auditoría

- **Registro de Actividades:**

  Configurar sistemas de logging y auditoría para registrar la conexión, el uso y la desconexión de dispositivos externos, permitiendo rastrear accesos no autorizados o comportamientos anómalos.

- **Alertas y Detección:**

  En niveles medios y altos, implementar soluciones de monitorización en tiempo real que generen alertas ante actividades sospechosas o intentos de conexión de dispositivos no autorizados.

Protección Física y Lógica

- **Protección Física:**

  Asegurar que los dispositivos externos se utilicen en entornos controlados. Por ejemplo, mantener áreas restringidas y controladas donde se conecten estos dispositivos, especialmente en casos de alta sensibilidad.

- **Actualización y Parcheo:**

  Garantizar que tanto los dispositivos como los sistemas a los que se conectan cuenten con las últimas actualizaciones y parches de seguridad.

Control de Acceso y Gestión de Dispositivos

- **Inventario y Registro:**

  Mantener un inventario actualizado de todos los dispositivos de almacenamiento externos que se conectan a la red, con registros de asignación y uso.

- **Autenticación y Autorización:**

  Establecer mecanismos de autenticación (por ejemplo, contraseñas robustas, autenticación multifactor) para el acceso a los datos almacenados en dispositivos externos, especialmente en entornos de nivel medio y alto.

- **Control de Puertos y Conexiones:**

  Implementar soluciones de gestión de dispositivos (MDM o software de control de puertos USB) que permitan autorizar únicamente dispositivos previamente registrados.

Actualmente encontramos distintas organizaciones con los puertos “apeados” deshabilitados, impidiendo así infecciones maliciosas, fuga de información, control sobre los datos… veamos algunas de las ventajas y desventajas sobre está práctica tan extendida:

Ventajas de Deshabilitar Puertos

Reducción de Riesgos de Malware y Exfiltración: Al limitar el uso de dispositivos externos, se disminuye la posibilidad de que se conecten medios infectados o se extraiga información sensible de forma no autorizada.

Control de Dispositivos No Autorizados: Restringir el uso de dispositivos extraíbles ayuda a garantizar que solo se usen aquellos autorizados y configurados conforme a las políticas de seguridad.

Consideraciones y Desafíos

Impacto en la Productividad: *Muchos empleados dependen de la conectividad a través de puertos USB o similares para actividades laborales legítimas (por ejemplo, transferencia de datos o conexión de periféricos autorizados). Deshabilitar estos puertos podría entorpecer el flujo de trabajo, por lo que es importante equilibrar la seguridad con la operatividad.*

*Flexibilidad y Excepciones**: En algunos casos, puede ser preferible implementar soluciones de control de dispositivos, que permitan registrar y autorizar conexiones específicas, en lugar de una desactivación total. Esto se alinea con la necesidad del ENS de aplicar medidas adaptadas al nivel de riesgo y a las necesidades del entorno.*

Estrategia Multicapa:

El ENS promueve un enfoque integral, por lo que la protección del perímetro no debe depender únicamente de la desactivación de puertos. Se recomienda combinarla con otras medidas, como el cifrado de datos, la gestión centralizada de dispositivos (MDM), monitorización de accesos y políticas de uso, para crear una defensa en profundidad.

Medidas Organizativas

Políticas y Procedimientos

- **Política de Uso de Dispositivos Externos:**

Definir y comunicar claramente las políticas de uso, estableciendo qué dispositivos pueden conectarse, en qué situaciones y bajo qué condiciones se permite el acceso a la información.

- **Procedimientos de Autorización:**

Establecer un proceso formal para la solicitud, revisión y autorización de dispositivos externos, asegurando que solo se utilicen aquellos que cumplan con los estándares de seguridad exigidos.

Formación y Concienciación

- **Capacitación Regular:**

Impartir programas de formación y concienciación sobre los riesgos asociados al uso de dispositivos externos, el correcto manejo de la información y las buenas prácticas de seguridad.

- **Simulacros y Evaluaciones:**

Realizar simulacros y evaluaciones periódicas para comprobar el cumplimiento de las políticas de seguridad y la correcta respuesta ante incidentes relacionados con dispositivos externos.

Gestión de Incidentes y Respuesta

- **Protocolos de Respuesta:**

Diseñar y documentar procedimientos específicos para la detección, análisis y respuesta ante incidentes que involucren dispositivos externos, incluyendo el borrado seguro de datos y la revocación de accesos.

- **Auditorías y Revisión Periódica:**

Realizar auditorías internas y externas de forma regular para verificar el cumplimiento de las medidas implementadas y detectar posibles áreas de mejora.

Control de Proveedores y Equipos

- **Evaluación de Proveedores:**

Asegurar que los proveedores de soluciones (como sistemas de cifrado o de gestión de dispositivos) cumplan con los estándares y directrices del ENS.

- **Actualización de Equipos:**

Garantizar que los equipos y dispositivos externos se sometan a revisiones periódicas para asegurar su integridad y la correcta aplicación de las medidas de seguridad.

Para trabajar de forma segura con dispositivos de almacenamiento externos, el **ENS recomienda** adoptar un *enfoque en capas* que combine medidas técnicas –omo el cifrado, el control de acceso, la monitorización y la protección física–con medidas organizativas, tales como políticas claras, formación, procedimientos de autorización y protocolos de respuesta ante incidentes. La implementación de estas medidas debe adaptarse a los diferentes niveles de seguridad (Básico, Medio y Alto), asegurando que en cada caso se minimicen los riesgos asociados a la utilización de dispositivos externos sin afectar la operatividad de la organización.

Jorge Noguerales Bautista

Coordinador del grupo de trabajo de IA y protección de datos