Mejores prácticas de Seguridad

Estas consideraciones e inquietudes habituales son inherentes al mundo de dispositivos conectados en el que vivimos. Ser consciente de ellas es el primer paso. El paso siguiente es implementar estas mejores prácticas en todos sus dispositivos conectados. Utilice esta lista como una guía de planificación.

1. Comience temprano

Haga planes pensando en la tecnología que se viene, y en cómo la protegerá.

2. Proteja los datos

Utilice conexiones encriptadas y autenticadas donde sea posible.

3. Controle los servicios

Considere desconectar los servicios tecnológicos que no planea utilizar.

4. Cambie las contraseñas

El uso de contraseñas predeterminadas facilita el acceso de los hackers a los dispositivos. **Active las contraseñas de interfaz de usuario.**

5. Administre su sistema de forma remota

Aproveche el sistema de administración remota segura para actualizar configuraciones rápidamente. Los dispositivos, soluciones y sistemas se vuelven blancos cada vez más fáciles cuanto más tiempo pasan con configuraciones obsoletas.

6. Habilite el registro de actividades

Utilice registros de actividad y auditoría cuando estén disponibles para detectar malos comportamientos.

7. Comparta solo lo imprescindible

Asegúrese de que los cronogramas y planes de actualización solo lleguen a manos de quienes los necesitan. Cuando demasiados empleados conocen los planes de actualización, aumentan las posibilidades de que se produzcan brechas de seguridad.

8. Monitoree los dispositivos “fuera de contacto”

Desarrolle un método para monitorear de forma continua su sistema y detectar dispositivos “fuera de contacto”. Cuando sospeche que se ha retirado un dispositivo, retenga sus credenciales hasta que confirme su ubicación.

9. Garantice capacidad de actualización

Elija dispositivos que puedan actualizarse durante su prolongada vida útil para mantenerse al día con los nuevos estándares. Asegúrese de que los sistemas de actualización puedan evitar la manipulación de los archivos de actualización.

10. Gestione el retiro de dispositivos

Planifique el retiro de dispositivos eliminando las configuraciones del sistema empresarial, borrando cuentas de usuario y credenciales de los dispositivos y comprobando que los sistemas existentes no estén codificados de forma rígida para buscar unidades retiradas.

11. Implemente el modelo CIA

Tenga en cuenta la confidencialidad, la integridad y la disponibilidad (CIA, por sus siglas en inglés) durante todas las etapas del ciclo de vida del dispositivo.

12. Implemente la planificación continua

Las actualizaciones de las prácticas de seguridad deben ser una prioridad continua. La planificación de la seguridad no es un evento único.

¿Sabía que...?

US$ 360.000

La encriptación minimiza los costos de la violación de datos en un promedio de **US$ 360.000**, por eso es la medida más efectiva contra el hackeo.[1]

81%

El uso de contraseñas robadas o débiles fue el causante del **81%** de las violaciones de datos relacionadas con el hackeo.[2]

US$ 1,2 millones

Las empresas que cuentan con equipos de respuesta ante incidentes de violación de datos y ponen a prueba los planes de respuesta reducen el costo de una violación en más de **US$ 1,2 millones.**[3]

38%

El **38%** de las empresas informaron haber tenido incidentes de seguridad que involucraron dispositivos empresariales.[4]

40%

El **40%** declara que los ataques cibernéticos son un factor que aumenta la importancia de proteger los dispositivos móviles.

197 días

Una organización tarda un promedio de 197 días en darse cuenta de que ha ocurrido una violación de datos.[5]

[1] Informe Cost of a Data Breach 2019, IBM Security • [2] 2017 Informe Verizon Data Breach Investigations, IBM Security • [3] Informe Cost of a Data Breach 2019 • [4] Informe Incident Response Threat Report, Carbon Black, noviembre de 2018 • [5] Informes Cost of Data Breach, 2018 y 2019, Instituto Ponemon