Prácticas idóneas de seguridad

Estas consideraciones y preocupaciones habituales son inherentes al mundo actual de dispositivos conectados. El primer paso consiste en tomar conciencia de ellas. El siguiente paso debe ser adoptar estas prácticas de sentido común para todos sus dispositivos conectados. Utilice esta lista de comprobación como guía de planificación.

1. Sea previsor

Planifíquese para la próxima tecnología y la protección que le proporcionará.

2. Proteja los datos

Utilice conexiones cifradas y autenticadas siempre que sea posible.

3. Controle los servicios

Plantéese la posibilidad de desactivar los servicios tecnológicos que no tenga previsto utilizar.

4. Cambie las contraseñas

La utilización de las contraseñas predeterminadas facilita a los hackers el acceso a los dispositivos. **Active contraseñas de interfaces de usuario.**

5. Gestión remota

Utilice un sistema seguro de gestión remota que le permita actualizar la configuración rápidamente. Cuanto más tiempo pasen los dispositivos, soluciones y sistemas con configuraciones desfasadas, más fácil resultará atacarlos.

6. Active el registro de la actividad

Utilice registros de actividad y auditoría si están disponibles para detectar comportamientos delictivos.

7. Necesidad de conocer

Mantenga las programaciones y planificaciones exclusivamente en manos de las personas que deban conocerlas. Cuantos más empleados conocen los planes de actualización, mayor es la probabilidad de que se produzcan infracciones de seguridad.

8. Supervise los dispositivos OOT

Desarrolle un método para supervisar la existencia en el sistema de dispositivos con los que se ha perdido el contacto (out-of-touch: OOT) Si sospecha que un dispositivo ha sido sustraído, retire sus credenciales hasta que confirme su ubicación.

9. Capacidad de actualización

Elija dispositivos que puedan actualizarse durante su prolongada vida de servicio para que estén al día en nuevos estándares. Asegúrese de que su sistema de actualización es capaz de prevenir la manipulación de los archivos de actualización.

10. Retirada de dispositivos

Planifique la retirada de dispositivos mediante la eliminación de la configuración de sistemas empresariales, la eliminación de cuentas/credenciales de usuarios de dispositivos y la comprobación de que los sistemas existentes no incorporan en su código la búsqueda de unidades retiradas.

11. C.I.D.

Tenga en cuenta la «Confidencialidad», la «Integridad» y la «Disponibilidad» durante todas las etapas del ciclo de vida de un dispositivo.

12. Planificación continua

La actualización de las prácticas de seguridad debe ser una prioridad constante. La planificación de la seguridad no es algo que se haga una sola vez.

¿Sabe que...?

360.000 $

El cifrado reduce el coste de las infracciones de la seguridad de los datos una media de **360.000 $**, lo que la convierte en la medida más efectiva contra los hackers.[1]

81 %

El uso de contraseñas robadas o débiles supone el **81 %** de las infracciones de seguridad de los datos relacionadas con la actividad de hackers.[2]

1,2 millones de $

Las empresas que cuentan con equipos de respuesta a incidentes de seguridad de los datos y con planes de respuesta reducen el coste de las infracciones de seguridad en más de **1,2 millones de $.**[3]

38 %

El **38 %** de las empresas informan de incidentes de seguridad que implican a dispositivos empresariales.[4]

40 %

El **40 %** señala que los ciberataques hacen que aumente la importancia de proteger los dispositivos móviles.

197 días

Una organización tarda una media de 197 días en descubrir que ha sufrido una infracción de la seguridad de los datos.[5]

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