DATA ASSURED

Consejos Cibernéticos

En colaboración con:

AMERICA'S SBDC DELAWARE | ANCHOR SECURITY

Presentado por:

AMERICA'S SBDC IOWA | Small Business Development Center

1 Proteger los dispositivos de endpoints frente a amenazas invisibles

Prepare los dispositivos para amenazas desconocidas dotándolos con herramientas de monitoreo como Watchdog de Anchor Security para proporcionar detección de anomalías, análisis de vulnerabilidades y respuesta activa para bloquear nuevas amenazas

2 Implementar un respaldo programado con control de versiones

En el caso de que los sistemas no puedan evitar la pérdida de datos o necesiten una versión anterior de un archivo, tener una copia de seguridad con control de versiones para todos los archivos importantes, le tranquilizara sabiendo que puede recuperar cualquiera de sus archivos en cualquier etapa de su vida.

Asegúrese de que el acceso a estos datos se controle en función del rol del usuario, de modo que los datos sólo sean accesibles por el personal requerido

3 Cree políticas sólidas de uso de seguridad para proteger a sus clientes y a sus empleados

La mejor manera de evitar el acceso de hackers es practicar el uso de dispositivos y servicios de maneras que los bloqueen por completo. La aplicación de la autenticación multifactor, las contraseñas de cadenas, el cifrado siempre que sea posible y un fuerte sentido común al revisar el correo electrónico pueden ir más allá de lo esperado.

Claramente defiene las consecuencias de violar dichas políticas

Haga que sus empleados sean responsables de cualquier dato confidencial que manejen o interactúen

Exija contraseñas seguras y aplique cambios frecuentes y significativos

4 Controle el acceso físico a los dispositivos

Garantizar la seguridad física es esencial. Los hackers que son capaces de obtener acceso físico son mucho más peligrosos que los

Requerir autenticación biométrica puede facilitar el manejo de contraseñas largas y tediosas, lo que aumenta la seguridad

5 Cifrar todas las conexiones, sin importar la necesidad

Esto no solo inspirará la confianza de sus clientes y consumidores, sino que también evitará muchos problemas imprevistos en el futuro.

Muestre al público que la seguridad es una prioridad para su empresa y su huella digital

6 Educar a los empleados

Asegúrese de que estén bien informados sobre las amenazas y cómo enfrentarlas.

Asegúrese, de que pueden seguir las políticas de uso de seguridad al disponer de los conocimientos necesarios, para realizar todas las acciones necesarias de forma segura.

7 Redes seguras

Su red suele ser la primera cosa que ven los hackers, y su primera línea de defensa. Asegúrese de que puede encargarse de cualquier cosa.

Implementar un IDS para detectar el uso malintencionado y anómalo de la red

Asegurarse de que las redes de invitados no funcionen con las redes corporativas

Utilice la lista blanca de direcciones MAC y el filtrado IP para asegurarse de que solo los dispositivos en los que confía estén en la red y que solo puedan comunicarse con los otros dispositivos que necesitan

Aislar los sistemas de pago a su propia red para que cualquier compromiso no signifique la pérdida tanto de los sistemas corporativos como de los sistemas de pago

IowaSBDC@iastate.edu

www.IowaSBDC.org

(515) 294-2030