Control de seguridad de 10 puntos

1 Compruebe si los parches están actualizados

Asegúrese de que sus servidores, PC, portátiles y dispositivos móviles están parcheados y actualizados. Esto debería incluir todas las aplicaciones, así como el sistema operativo y el firmware. Es buena idea utilizar una solución de gestión de parches y activar las actualizaciones automáticas siempre que sea posible.

Asegúrese de que los servicios orientados a la web están parcheados para las vulnerabilidades de seguridad conocidas. Los servicios de este tipo que permanecen sin parches pueden representar un riesgo muy alto y son susceptibles de ser blanco de los atacantes. También debe comprobar los argumentos comerciales y los factores atenuantes de los sistemas sin parches conocidos en relación con el aumento de la amenaza.

2 Compruebe los controles de acceso y la política de contraseñas

Asegúrese de que todos los usuarios utilizan contraseñas únicas que no se utilizan en otras cuentas personales. Pídale a los usuarios que comprueben que sus contraseñas son seguras y haga que cambien las que no lo sean de inmediato. Los gestores de contraseñas son una forma excelente de mantener contraseñas fuertes y únicas. Si la autenticación multifactor (MFA) está disponible, asegúrese de que está activada.

Asegúrese de revisar las cuentas que tienen acceso privilegiado o administrativo y elimine las cuentas antiguas, las que no se utilicen o no se reconozcan. Las cuentas con privilegios pueden ser administradores del sistema, pero también pueden ser cuentas que tengan acceso a sistemas o información sensibles.

Seguir el principio «del menor privilegio» es la mejor política a la hora de gestionar los controles de acceso.

3 Compruebe sus defensas

Asegúrese de que el software antivirus está instalado en todos los ordenadores personales y portátiles, y compruebe periódicamente que está activo en todos los sistemas y que las firmas están actualizadas. Vuelva a comprobar que las reglas de su cortafuegos son las esperadas. En particular, debe comprobar si hay normas temporales que puedan haberse dejado en vigor más allá de su uso previsto.

4 Comprobar el registro y la supervisión

Revise los registros que tiene establecidos. Comprueba cómo se protegen los registros y cuánto tiempo se conservan. Deben mantenerse durante un mes como mínimo.

Durante el periodo de mayor riesgo, debería considerar aumentar la frecuencia con la que comprueba los registros de seguridad de los servidores y dispositivos de red. Una solución de gestión de registros o SIEM ayudará mucho en este proceso.

5 Compruebe su estrategia de copia de seguridad y recuperación

Confirme que sus copias de seguridad funcionan correctamente y que dispone de un plan de recuperación documentado. Compruebe que se ha realizado recientemente una prueba de recuperación para tener la seguridad de que se recuperará de una pérdida del sistema.

Las pruebas de recuperación son importantes, ya que a menudo revelan suposiciones incorrectas sobre cómo funcionará la recuperación a partir de copias de seguridad. La prueba de recuperación debe comprobar además que las dependencias críticas, aparte de los datos, también pueden recuperarse, como las claves privadas y los tokens de acceso.

6 Compruebe su plan de respuesta a incidentes

Revise su plan de respuesta a incidentes y compruebe que está actualizado. Compruebe que los planes de notificación y los datos de contacto correspondientes son correctos. Asegúrese de que queda claro quién tiene autoridad para tomar decisiones clave, tanto dentro como fuera del horario laboral, si se trata de otras personas.

Su plan de respuesta a incidentes debe estar a disposición de todos los que puedan necesitarlo, tanto si están en la oficina como si trabajan a distancia.

7 Compruebe sus conexiones a Internet

Compruebe que los registros de sus conexiones a Internet están actualizados. Esto debería incluir factores como qué direcciones IP utilizan sus sistemas en la web y qué nombres de dominio pertenecen a su organización. Los datos de registro de dominios deben conservarse de forma segura. Su cuenta de registro de dominio debe tener una contraseña segura y MFA, si está disponible.

Realice un escaneado externo de vulnerabilidades de todas sus conexiones a Internet y compruebe que se ha parcheado todo lo necesario.

8 Compruebe su capacidad de respuesta al phishing

Educar a los usuarios sobre cómo reconocer probables intentos de phishing y otras formas de ingeniería social debería formar parte de su plan de formación sobre concienciación en materia de seguridad. Asegúrese de que el personal sabe cómo informar de correos electrónicos de phishing y de que dispone de un proceso para tratar cualquier incidente de seguridad que se notifique.

9 Comprobar el acceso de terceros

Si necesita que terceras organizaciones tengan acceso a sus sistemas, asegúrese de tener claro qué nivel de privilegio se extiende a sus sistemas y quién lo controla.

En una época de mayor riesgo cibernético, debe asegurarse de eliminar cualquier acceso que ya no sea necesario.

Antes de permitir la conexión, debe revisar las prácticas de seguridad de los terceros en cuestión. Los ataques a la cadena de suministro han sido un vector de amenaza en rápido aumento en los últimos tiempos.

10 Comprobar las fuentes de información sobre amenazas

Mantenerse al día de las amenazas relevantes durante un periodo de aumento del riesgo cibernético es fundamental para evitar y responder a los riesgos de seguridad.

Hay muchas fuentes excelentes de información sobre amenazas, pero una buena fuente por defecto es el sitio web del National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk/). Puede ir más allá y registrarse para obtener una cuenta NCSC CiSP a través de la cual podrá acceder y compartir información sobre amenazas con otras organizaciones, así como recibir actualizaciones inmediatas.
También es posible inscribirse en el Early Warning Service (servicio de alerta temprana) del NCSC en https://www.ncsc.gov.uk/information/early-warning-service para que la organización pueda informarle de cualquier actividad maliciosa procedente de sus sistemas