Diligent

10 PREGUNTAS

que hacerse al evaluar la seguridad de los portales para juntas directivas

Cuando las organizaciones contratan proveedores de portales para juntas directivas, les están confiando la custodia de documentos confidenciales y el sistema para administrar el acceso a esos documentos. Esta confianza va más allá de las especificaciones técnicas. Esa es la razón por la cual es esencial que las juntas directivas, secretarios generales, consultorías jurídicas y CIOs se sientan cómodos y confiados en la seguridad del proveedor de portales para juntas directivas.

Con este propósito, a continuación encontrará 10 preguntas que las organizaciones deben hacer acerca de cualquier proveedor potencial de portales para juntas directivas:

1 ¿Realiza el proveedor inversiones importantes en investigación y desarrollo de ciberseguridad?

Las amenazas de ciberseguridad están en constante evolución, no solamente debido a los avances en tecnología, sino también debido a los cambios en el mundo cibernético. Los piratas solitarios han dado paso a organizaciones sofisticadas que pueden causar perturbaciones a una escala global. Un proveedor de portales para juntas directivas debe ser capaz de demostrar las capacidades de investigación y desarrollo que le permitan mantenerse a la vanguardia de las nuevas amenazas.

2 ¿Es el proveedor transparente acerca de sus procesos de seguridad?

El proveedor debe explicar claramente sus controles de seguridad física (protección de los servidores, enrutadores y otros equipos), los procesos de selección para los nuevos empleados, los controles internos, supervisión del sistema (si tuvieran un ataque de piratas, ¿cómo lo sabrían?) y cualquier historial de violaciones de seguridad y su resolución.

3 ¿Cumple el proveedor con los más altos estándares de la industria?

Como terceros manipuladores de información confidencial, los portales de las juntas directivas deben cumplir con normas de seguridad comparables a los de los departamentos de TI más exigentes en todas las industrias. Las acreditaciones claves incluyen: un historial impecable de auditorías SOC/SSAE 16 anuales (que cubren cómo los proveedores informan sobre sus controles internos) y la certificación de seguridad ISO 27001 (cumplimiento de los sistemas de seguridad de información del proveedor de software real con las normas internacionales, en lugar del cumplimiento de sus centros de alojamiento de datos simplemente).

4 ¿Permite el proveedor pruebas de penetración externa?

La mayoría de los proveedores de portales para juntas directivas realizan pruebas de penetración como parte de su control de calidad. Los portales con altos estándares de seguridad realizarán pruebas de manera casi continua en lugar de anualmente con el fin de mantenerse al día con las amenazas en evolución. Además, deben permitir a los clientes y potenciales clientes realizar sus propias pruebas de seguridad (o que contraten a terceras partes de su preferencia) para ejecutar pruebas independientes. Si lo hacen, están dando muestras de una poderosa confianza (así como reconociendo que la seguridad es en última instancia un esfuerzo de equipo).

5 ¿Confía el proveedor en las plataformas o software de terceros?

Muchos de los portales para juntas directivas se construyen en función de las plataformas disponibles comercialmente o usan componentes listos para usar para ciertos elementos de su software. Sin embargo, esos elementos de terceros vienen con sus propias vulnerabilidades de seguridad, las cuales son atractivas para los piratas precisamente porque el uso de esas plataformas es tan generalizado y no han sido diseñados para satisfacer las exigencias de un portal para juntas directivas. En cambio, los portales para las juntas deben construirse desde la base hacia arriba, con características de seguridad incorporadas por diseño a las aplicaciones en cada punto.

6 ¿Qué nivel de seguridad física proporciona el proveedor?

Si bien la información digital a menudo se considera intangible, se almacena de hecho en servidores muy reales. Esas instalaciones de alojamiento de datos deben protegerse con defensas de seguridad en sitio, televisión de circuito cerrado y múltiples capas de seguridad perimetral. Los servidores mismos deben protegerse en cajas especiales seguras y los datos almacenados de cada organización deben contar con segregación y encriptación lógicas. Y las claves criptográficas de estos servidores se deben proteger mediante dispositivos resistentes y a prueba de manipulaciones.

7 ¿Qué grado de redundancia de datos se ofrece?

¿Están los datos respaldados y los centros de datos principales dotados de procedimientos de falla segura hacia centros de datos de recuperación por desastres? Los proveedores de portales para juntas directivas deben ofrecer ubicaciones remotas y geográficamente dispersas para garantizar que cualquier evento que impacte en una ubicación no afectará la segunda ubicación. Además, la redundancia de datos debe respaldarse con inteligencia permanente, en tiempo real sobre el rendimiento de los datos.

8 ¿Puede el acceso al portal restringirse a un dispositivo específico?

Con los miembros de las juntas directivas repartidos en todo el mundo y viajando frecuentemente, la necesidad de asegurar sus dispositivos móviles es de suma importancia. ¿Puede el acceso al portal de un usuario restringirse a un dispositivo específico que está registrado en el portal para juntas directivas? ¿Existe también una opción para desactivar el acceso por navegador? Las soluciones de autorización de dispositivos permiten a las organizaciones evitar el acceso a dispositivos desconocidos y no confiables. El resultado es un mayor control de derechos de acceso y de ubicaciones.

9 ¿Le permite el proveedor asignar el nivel adecuado de seguridad del portal?

Cada solución de seguridad implica una relación de compromiso entre conveniencia y seguridad. Como consecuencia, un tamaño único definitivamente no se ajusta a todas las organizaciones. En cambio, un portal para juntas directivas debe adaptar las funciones con el fin de ajustarse a las necesidades de seguridad específicas de la organización, tal como permitir fortalezas de contraseñas diferentes, políticas de bloqueo y opciones para exportar e imprimir documentos de la junta directiva desde los portales.

10 ¿Son respaldadas las características de seguridad del portal con soporte al cliente?

No importa cuán fuerte pueda ser la seguridad de un portal, la supervisión humana es necesaria para garantizar que cualquier problema sea resuelto con prontitud. Por ejemplo, un director que repetidamente escribe mal la contraseña y cuyo acceso al sistema es bloqueado debe recibir una llamada de soporte al cliente tanto para brindarle soporte como para comprobar la causa de sus intentos fallidos.

Para mayor información o solicitar una demostración, comuníquese con nosotros hoy:

Llame: + 1 973 939 9404

Correo electrónico: info@diligent.com

Visite: www.diligent.com

C0116_ES