¿Qué es BCP (Business Continuity Plan, Plan de continuidad comercial)?

¿Qué es BCP (Business Continuity Plan, Plan de continuidad comercial)? Siempre es importante prepararse para el peor de los casos. El hecho de que nos centremos en crear soluciones de TI confiables no significa que no pensemos en lo que sucedería en el peor de los casos. La preparación es clave, por lo que siempre consideramos las opciones de continuidad comercial de nuestros clientes y ayudamos a asegurarnos de que sean adecuadas para su propósito.

Protegiendo su negocio del malware

A pesar de que la tecnología de software y hardware ha mejorado, es muy probable que un bloqueo de datos afecte a la mayoría de los propietarios de datos. Ya sea debido a un error físico, un sistema de archivos corrupto o un error del usuario, las consecuencias de un bloqueo de datos pueden ser catastróficas.

En 2018, el FBI reportó 1,493 casos de ransomware con una pérdida total de $ 3,621,857. Han aparecido nuevas formas de ransomware a un ritmo alarmante, siendo las más recientes SamSam, CrypoFortress y TeslaCrypt.

La mejor manera de proteger su negocio del ransomware es tener una copia de seguridad segura y eficiente. Debe probar su copia de seguridad regularmente para asegurarse de que funciona de manera óptima de esa manera puede obtener acceso a sus datos de copia de seguridad rápidamente cuando sea necesario.

Lo que significa

Un BCP analiza el panorama general y considera mucho más que solo su infraestructura tecnológica.
La planificación de continuidad del negocio (BCP) es el proceso planificado para prevenir y recuperar posibles amenazas a un negocio. Además de prevenir, el objetivo de BCP es habilitar las operaciones continuas antes y durante la ejecución de su plan de recuperación ante desastres.

Un BCP es un plan documentado que establece los pasos a seguir cuando una organización se ve afectada por escenarios inesperados que a menudo son críticos para el negocio. Un buen BCP cubre la necesidad de recursos, procesos y funciones para volver a la operación normal, reduciendo la cantidad de tiempo de inactividad.

La planificación de la continuidad del negocio (BCP) es el proceso involucrado en la creación de un sistema de prevención y recuperación de amenazas potenciales para una empresa. El

plan garantiza que el personal y los activos estén protegidos y puedan funcionar rápidamente en caso de desastre. El BCP generalmente se concibe de antemano e involucra aportes de partes interesadas y personal clave.

BCP implica definir todos y cada uno de los riesgos que pueden afectar las operaciones de la compañía, convirtiéndolo en una parte importante de la estrategia de gestión de riesgos de la organización. Los riesgos pueden incluir desastres naturales (incendios, inundaciones o eventos relacionados con el clima) y ataques cibernéticos . Una vez que se identifican los riesgos, el plan también debe incluir:

- Determinar cómo esos riesgos afectarán las operaciones
- Implementar salvaguardas y procedimientos para mitigar los riesgos.
- Procedimientos de prueba para asegurar que funcionan
- Revisar el proceso para asegurarse de que esté actualizado

Los BCP son una parte importante de cualquier negocio. Las amenazas y las interrupciones significan una pérdida de ingresos y costos más altos, lo que conduce a una caída en la rentabilidad. Y las empresas no pueden confiar solo en el seguro porque no cubre todos los costos y los clientes que se trasladan a la competencia.

Comprensión de la planificación de continuidad del negocio (BCP)

Las empresas son propensas a una serie de desastres que varían en grado de menor a catastrófico. La planificación de la continuidad del negocio generalmente está destinada a ayudar a una empresa a continuar operando en caso de desastres importantes como incendios. Los BCP son diferentes de un plan de recuperación ante desastres, que se centra en la recuperación del sistema de TI de una empresa después de una

crisis.

Considere una compañía financiera con sede en una ciudad importante. Puede poner un BCP en su lugar tomando medidas que incluyen hacer una copia de seguridad de su computadora y los archivos del cliente fuera del sitio. Si algo le sucediera a la oficina corporativa de la compañía, sus oficinas satélite aún tendrían acceso a información importante.

Un punto importante a tener en cuenta es que BCP puede no ser tan efectivo si una gran parte de la población se ve afectada, como en el caso de un brote de enfermedad.

Desarrollo de un plan de continuidad comercial

Hay varias medidas que muchas empresas deben seguir para desarrollar un BCP sólido. Incluyen:

- Análisis de impacto empresarial : aquí, la empresa identificará funciones y recursos relacionados que son urgentes. (Más sobre esto a continuación).
- Recuperación : en esta parte, la empresa debe identificar e implementar pasos para recuperar funciones empresariales críticas.
- Organización : se debe crear un equipo de continuidad. Este equipo elaborará un plan para gestionar la interrupción.
- Entrenamiento : El equipo de continuidad debe ser entrenado y probado. Los miembros del equipo también deben completar ejercicios que repasen el plan y las estrategias.

Las compañías también pueden encontrar útil elaborar una lista de verificación que incluya detalles clave como información de contacto de emergencia, una lista de recursos que el equipo de continuidad pueda necesitar, donde se almacenan o almacenan

datos de respaldo y otra información requerida, y otro personal importante.

Además de probar el equipo de continuidad, la compañía también debe probar el BCP. Debe probarse varias veces para garantizar que se pueda aplicar a muchos escenarios de riesgo diferentes . Esto ayudará a identificar cualquier debilidad en el plan que luego pueda identificarse y corregirse.

Ejemplo

Escenario potencial: recuperación de una inundación

Imagine que su oficina ha sufrido una inundación, permanecerá inaccesible durante meses, ¿cómo continuará?
Un buen plan de continuidad comercial cubrirá todos los incidentes significativos. Tales como fuego, robo, inundación y ciberataque. También tendrá un plan para la pérdida de un sistema crítico. Al pensar en un buen BCP, debe pensar en lo siguiente:

- Espacio de oficina
- Sistemas de TI
- Telecomunicaciones
- Correo y entregas
- Acceso de empleados

Debe tener un (BCP) y un (DRP)

Un DRP es un proceso documentado para reconstruir la infraestructura de TI de una empresa después de un incidente.

Seis puntos críticos que debe cubrir en

su DRP y BCP

Un buen BCP / DRP debe incluir todos los tipos posibles de incidentes y escenarios, por ejemplo, errores humanos, desastres naturales, ataques de piratería.
Involucre a todos los empleados relevantes al preparar su BCP y DRP; esto asegurará que el proceso sea completo y que se cubran aspectos probables.

Ponga a prueba sus planes regularmente. Las pruebas mostrarán sus debilidades y lo ayudarán a equipar a su organización para el día en que suceda algo dramático.

Como es fundamental para una empresa mantener sus sistemas actualizados con nuevas versiones y licencias, lo mismo ocurre con los planes. Los planes deben actualizarse y mantenerse continuamente. No es raro que un BCP y DRP tengan cientos de páginas, por lo que es una buena idea dividirlo en partes relevantes, lo que facilita su orientación.

Asegúrese de documentar su plan por escrito y guárdelo en un lugar seguro. Puede parecer simple, pero cuando todo el mundo está en estado de pánico, tener que buscar alrededor de las instalaciones comerciales para su BCP / DRP es lo último que querrá hacer.

Asegúrese de establecer contacto con un socio de recuperación de datos y mantener sus detalles en su DRP. Tener una empresa de recuperación de datos en marcación rápida podría marcar la diferencia en una situación urgente.

Leer también: Post anterior de DRP; Colocation (Colocación) debe ser parte de su plan de recuperación de desastres; Recuperación de desastres como servicio (DRaaS); ventajas y desventajas; Backup remoto, qué es y por qué es importante