Noviembre 2025

BOLETÍN INFORMATIVO

Acerca de Chubb

Con operaciones en 54 países y territorios, Chubb ofrece seguros comerciales y personales de propiedad y accidentes, accidentes personales y seguro médico complementario, reaseguro y seguro de vida a un grupo diverso de clientes. Como empresa de suscripción, evaluamos, asumimos y gestionamos el riesgo con conocimiento y disciplina. Atendemos y pagamos nuestros reclamos de manera justa. La compañía también se define por su amplia oferta de productos y servicios, amplias capacidades de distribución, solidez financiera excepcional y operaciones locales a nivel mundial. La empresa matriz Chubb Limited cotiza en la Bolsa de Valores de Nueva York (NYSE: CB) y es un componente del índice S&P 500. Chubb mantiene oficinas ejecutivas en Zurich , Nueva York , Londres , París y otras ubicaciones, y emplea aproximadamente a 33.000 personas en todo el mundo.

No juegues al dominó con los ciber riesgos de tu empresa

Los riesgos de ciber seguridad son especialmente desafiantes para las empresas, pues tienen el potencial de causar severas disrupciones en el negocio y además tienen un alto impacto financiero.

Comprender estos riesgos y cómo funcionan los ciberataques puede ayudarte a mantener a raya a los hackers, estar mejor preparado y proteger a tu empresa.

El efecto dominó

Pocas veces se entiende, antes de un ciberataque, que el impacto de este tipo de incidentes puede crear un espiral negativo. A medida que una empresa se ve progresivamente afectada, los costos de reparación escalan con rapidez.

La primera pieza del dominó: costos por pérdidas de negocios. Cuando el sitio web o los sistemas computacionales son atacados y retirados de la red, las tiendas virtuales pueden resultar inutilizables para los clientes, y las transacciones pueden no poder ser procesadas. Si bien las tiendas físicas pueden seguir abiertas, con la tienda virtual fuera de servicio, los clientes pueden ir a otros lugares.

Segunda pieza: costos reputacionales y pérdida de clientes. Si la información personal de los clientes (como los números de sus tarjetas de crédito) es robada, la confianza del consumidor se ve sacudida. La brecha puede ser agravada por la mala prensa, que puede mutilar la reputación de marca y llevar a una devastadora deserción por parte de los clientes.

Tercera pieza: costos de restauración.
Luego de un ciberincidente, surge una serie de tareas —como restaurar los softwares, los sistemas computarizados y las bases de datos digitales— que requieren de tiempo, dinero, personal y, muchas veces, costosos recursos externos.

Cuarta pieza: costos legales y de liquidación.
Cuando un ciberataque impacta negativamente a los consumidores, vendedores, proveedores u otros, puede haber ramificaciones legales. Las demandas pueden ser extremadamente costosas y consumir mucho tiempo.

Cuando estas piezas comienzan a caer, los crecientes costos pueden incluso llevar a una empresa a la quiebra.

Cómo acceden los cibercriminales

Hay muchas maneras en las que los cibercriminales pueden tener acceso al sitio web de una empresa o a los servidores internos para robar datos o atacar a la compañía. Entre estas se incluyen:

Artículos electrónicos como computadores o tablets, con acceso legítimo a los servidores, que no cuentan con políticas de seguridad adecuadas.
Uso extendido de claves débiles por parte de los empleados y políticas corporativas poco exigentes para la creación de claves.
Tomar ventaja de fallas en la fuente de poder o el acceso a internet (las que pueden o no haber sido causadas por personas con malas intenciones).
Ataques activos que explotan las falencias de seguridad y a menudo emplean programa maligno o sofisticadas técnicas como el ransomware, el phishing o credential stuffing (relleno de contraseñas).

Protegiendo a tu empresa de un ciberataque

Aunque detener a los cibercriminales pueda parecer una tarea compleja, hay un medidas simples que las compañías pueden tomar para crear su propio programa de administración del ciberriesgo y así limitar su exposición.

Actualiza los equipos de TI y softwares de seguridad. Los computadores y sistemas operativos obsoletos o sin actualización pueden ser fácilmente violados por cibercriminales.

Monitorea las redes. Las compañías pueden limitar los daños cuando las anormalidades son detectadas rápidamente. Un experto en ciberseguridad puede identificar áreas de alto riesgo. También hay softwares de seguridad que ofrecen soluciones de monitoreo.

Educa a los empleados sobre ciberseguridad. Según un estudio de Chubb, solo el 31% de quienes contestaron reporta que su empleador les entrega anualmente un programa con entrenamiento y actualización sobre ciberseguridad. Asegúrate de que tu personal entienda el importante rol que cumple en la prevención de un ciberataque y ayúdale a establecer hábitos positivos y seguros mediante políticas de ciberseguridad escritas y reforzadas, además de una capacitación regular.

Exige una buena “higiene de claves”. Esto es un asunto central en cualquier programa de ciberseguridad. Las claves debieran ser fuertes (por ejemplo, una mezcla de letras, números y símbolos) y cambiarse con frecuencia. Cuando los empleados dejan la compañía, sus credenciales debieran ser automáticamente revocadas.

Crea un plan de respuesta para ciber incidentes. Algunos incidentes pueden ser mitigados con un plan de respuesta previamente preparado y un equipo de respuesta tanto interno como externo. Con una estrategia y los expertos ya preparados, la respuesta y la resolución de cualquier ciber incidente puede ocurrir con mayor rapidez.

Adquiere un seguro para ciber incidentes. Si bien las medidas proactivas son esenciales, un plan de respaldo actúa como un salvavidas contra el ciber riesgo. Un buen plan de seguros para ciberataques es más que una herramienta para mitigar costos financieros: puede ayudar a la empresa a entender mejor cómo estar preparada para un incidente de este tipo y ofrecer recursos y colaboradores, como —por ejemplo— capacitadores en ciberseguridad para los empleados.