Enero 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.

“5 consejos cibernéticos claves para pymes “

Asegurarse de que los antivirus y otro software de seguridad estén al día es solo el punto de partida. Las pymes pueden hacer mucho más para reducir el riesgo de enfrentarse a un ciberataque.

Chubb recomienda seguir los siguientes pasos de mitigación:

Ojo con las claves

Deben estar compuestas por una mezcla de letras, números y símbolos que se cambien de manera frecuente.

Una de las maneras más simples que los ciber criminales tienen para acceder a los activos de una pyme es cruzar la “puerta abierta” virtual que los colaboradores proveen cuando usan claves débiles. Por eso es recomendable que las pymes establezcan por escrito una política que exija claves sólidas, las cuales deben cambiarse con frecuencia. Cuando los colaboradores se van de la compañía, las claves debieran cambiarse automáticamente o las cuentas marcarse como inactivas.

Capacitar en ciber seguridad

Hay que enseñarles a los empleados a estar ciber alertas.

Las pymes deberían hacer saber a sus colaboradores que ellos también son parte de la prevención de ciber ataques en la compañía. Es demasiado fácil que un software malicioso entre en el servidor de la compañía cuando las laptops de la compañía y otros dispositivos son usados fuera del recinto y luego conectados a la red interna.

La mejor manera de establecer hábitos positivos y seguros es por medio de educación y capacitación regularmente planificada.

Asimismo, es necesario restringir el acceso a información sensible, permitiendo que tengan acceso a ella solo los administradores o quienes la requieran para operaciones de la compañía.

Actualizaciones y software de seguridad

Incluso las ofertas básicas de seguridad presentan tecnologías similares a las usadas por las grandes empresas.

Computadoras y sistemas operativos obsoletos pueden ser un riesgo porque son vulnerables a las técnicas de hackeo más sofisticadas y a nuevas formas de malware. Es importante que las pymes monitoreen a aquellos que tienen acceso autorizado a la red y a la red misma. A pesar de que las pymes usualmente no tienen expertos en seguridad dentro de su organización, es posible acceder a ofertas de software básicos que se pueden descargar e implementar, en cosa de minutos, y que son las mismas soluciones tecnológicas utilizadas por grandes empresas.

Plan de respuesta

Con proveedores internos, externos o ambos.

Las pymes deben tener un plan de respuesta frente a ciber emergencias. No es indispensable que sea un costo fijo extra: pueden participar tanto los colaboradores como proveedores externos de servicios. El foco debe estar siempre en la rapidez de la respuesta.

Adquirir un ciber seguro

Esto ayuda a cubrir de manera más completa los activos y flujos de caja.

El costo de los seguros será siempre mucho menor al costo de cerrar un negocio como consecuencia de uno o más ciber ataques.

CHUBB®