07/11/2025

Por qué la ciberseguridad es esencial para las pequeñas empresas

La ciberseguridad debe abordarse como parte de la gestión diaria de riesgos

El Mes de la Concientización sobre la Ciberseguridad nos recuerda que los riesgos que enfrentan los empresarios hoy en día son muy diferentes a los de hace unos años. Los intentos de fraude ya no son simples ni oportunistas. Se han vuelto más inteligentes, más específicos y están impulsados por nuevas tecnologías como la inteligencia artificial (IA).

Para las pequeñas empresas, esto representa un desafío único que no pueden permitirse ignorar. Si bien es posible que no se consideren objetivos prioritarios, los ciberdelincuentes ven a las pequeñas empresas como puntos de entrada privilegiados porque podrían carecer de los mismos recursos defensivos que las instituciones más grandes. Pero seamos claros: la resiliencia no se trata de tamaño; se trata de enfoque y preparación. Su banco es un aliado en esta lucha, pero la primera línea de defensa contra pérdidas financieras comienza con ti.

Los intentos de fraude siguen aumentando

Los intentos de fraude han pasado de ser ataques aleatorios puntuales a estrategias a largo plazo de varias etapas. Como se compartió recientemente en el Informe sobre el Estado del Fraude 2025 de Alloy , el 71 % de los intentos de fraude actuales son cometidos por bandas de crimen organizado. Los ciberdelincuentes pueden robar datos hoy y atacar meses o incluso años después. Dado que la frecuencia de las estafas bancarias ha aumentado un 65 % en el último año , ahora es más importante que nunca comprender cómo han avanzado los ataques y qué debes tener en cuenta para proteger tu negocio.

Los estafadores ahora pueden imitar el identificador de llamadas de una empresa, crear réplicas de sitios web y facturas legítimas, e incluso imitar una voz conocida. Todo esto para generar confianza y legitimidad y obtener información confidencial. Esto incluye hacerse pasar por empresas con las que podría trabajar, incluyendo a sus proveedores y su banco. La suplantación de identidad empresarial se ha convertido en una de las formas más realistas y efectivas de phishing, ya que se basa en el instinto: primero entrar en pánico, luego pensar. Si bien la IA ayuda a que estos esquemas parezcan auténticos, la primera defensa es la consciencia y la interpretación de las señales. Si algo «parece extraño», probablemente lo sea.

Cómo construir controles más fuertes

Toda empresa debe evaluar periódicamente cómo se gestionan las transacciones, qué empleados y proveedores tienen acceso a sistemas sensibles y qué controles existen para detectar actividades sospechosas. Es igualmente importante crear un entorno donde los empleados comprendan su función y se sientan capacitados para proteger la empresa.

Capacitar a los empleados para detectar señales de alerta y saber cuándo escalar se convierte en un activo colectivo; y el liderazgo marca la pauta. La ciberseguridad debe abordarse como parte de la gestión diaria de riesgos, no como un problema informático ocasional. Las empresas más seguras son aquellas que trabajan en equipo para mantenerse alertas.

Las relaciones sólidas con las instituciones financieras son fundamentales. Contar con un banquero o asesor de confianza que comprenda el negocio y pueda identificar actividades irregulares es invaluable. El fraude ya no es una cuestión de «si» sino de «cuándo», y esas conexiones personales permiten respuestas más rápidas y coordinadas ante emergencias.

Ve más allá de los métodos de pago obsoletos

Para mantenerse protegidos, los líderes empresariales necesitan repensar y comprender cómo se mueve el dinero en sus organizaciones y las posibles fallas de sus procesos. Las herramientas financieras modernas no solo son más accesibles y convenientes, sino que también ofrecen mayor protección. En conjunto, estos métodos brindan a las pequeñas empresas el mismo nivel de sofisticación y protección que antes solo estaba disponible para instituciones más grandes. Por ejemplo:

- Las transferencias ACH y bancarias protegidas con autenticación multifactor verifican cada transacción antes de que se muevan los fondos.
- Positive Pay ayuda a detectar cheques alterados o falsificados antes de que se procesen.
- Las plataformas de pago de facturas protegen los detalles de las cuentas y crean un entorno controlado para los pagos de rutina.

Los bancos están inmersos en esta evolución, colaborando con las empresas para reforzar sus defensas. Entre bastidores, los bancos supervisan el comportamiento de las transacciones, verifican las credenciales comerciales y detectan anomalías mediante protocolos internos. Si bien estos pasos adicionales pueden engordar la apertura de cuentas o los controles de seguridad, son medidas esenciales para la seguridad de las empresas.

Los dueños de negocios deben tomarse el tiempo para hacer preguntas, revisar sus productos financieros y evaluar el funcionamiento de sus procesos. La simple constancia en estas prácticas puede determinar si un intento de vulneración se convierte en un inconveniente menor o en una interrupción importante.

Tenga un plan de recuperación y resiliencia cibernética

Cuando ocurre un ataque, la rapidez es fundamental. Contactar a tu banco, congelar las cuentas comprometidas, cambiar las credenciales y documentar cada paso puede ayudar a los investigadores e instituciones financieras a contener la amenaza y comenzar la recuperación. Los mejores resultados se obtienen al saber qué hacer antes de que ocurra un incidente.

Incluso las organizaciones mejor preparadas pueden sufrir un ciberataque. Lo que distingue un daño duradero de una interrupción temporal es la eficiencia con la que una empresa responde. Un plan de recuperación claro y viable debe identificar qué sistemas son críticos, a quién contactar de inmediato (recuerde a su banco) y cómo reanudar las operaciones rápidamente. Para los líderes empresariales, el objetivo no es eliminar el riesgo, sino gestionarlo con cuidado, proteger lo construido y garantizar que la innovación y el crecimiento continúen con confianza. El futuro de su negocio depende de ello.

Fuente: https://forbes.es/

LINK DE LA NOTICIA