LITORALPRESS

Fecha: 30-11-2024
Medio: Revista Channel News
Supl. : Revista Channel News
Tipo: Noticia general
Título: Protección contra fraudes y violaciones de datos

Pág. : 37
Cm2: 414,0
VPE: $ 571.767

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

Control de accesos

Protección contra fraudes y violaciones de datos

Por Ricardo Arellano, Senior Manager Application Security de Cybertrust Latam.

La transformación digital no es exclusiva de las grandes empresas. Las Pymes también tienen la oportunidad de reinventarse e integrar la tecnología en sus procesos para mejorar su competitividad. Sin embargo, para que la digitalización genere valor real, es esencial incorporar ciberseguridad desde el principio.

Actualmente, las violaciones de datos están en aumento y ninguna organización está a salvo de ciberataques, fugas o manipulaciones de información. Esto se debe, en parte, a la movilidad de la fuerza laboral y al uso creciente de servicios en la nube, que ponen muchas cargas de trabajo fuera del alcance de las redes corporativas tradicionales.

El Centro Criptológico Nacional de España emitió recientemente un informe que indica que 80% de los ciberataques está dirigido a los empleados. Esta tendencia no se limita a España, sino que también afecta a Chile y al resto del mundo. Los empleados continúan siendo el eslabón más vulnerable en la cadena de seguridad de la información. Por este motivo, adoptar medidas de control de acceso que limiten estrictamente las funciones a las que los colaboradores pueden acceder es clave. La falta de controles adecuados permite que algunos usuarios se salten procesos internos, lo que pone en riesgo a la organización.

Existen normativas y estándares que guían las mejores prácticas en gestión de accesos: ISO 27002 (un marco clave para la gestión de la seguridad de la información); Políticas de Control de Acceso (Ministerio del Interior de Chile); la Ley 19.223 (sobre delitos informáticos); Ley 19.628 (de protección de datos personales) y el Reglamento Europeo de Protección de Datos (GDPR). El común denominador en todas estas normativas es la prevención de fraudes y la protección de los activos de información.

Alternativas para la gestión de acceso

Algunas encuestas corporativas muestran que 8 de cada 10 empresas han sufrido fraudes en el último año, de los cuales el 61% fue detectado por controles internos. Sin embargo, solo un 12% de las empresas que sufrió fraudes implementó medidas preventivas después del incidente.

Para reducir la probabilidad de violaciones de datos o fugas de información, las empresas deben implementar acciones concretas para mejorar el control interno, entre las cuales se incluyen limitar el uso de cuentas, asignar accesos solo para las funciones esenciales; otorgar accesos según el cargo, definir roles claros para cada puesto; implementar soluciones de Identity Management; facilitar la gestión de identidades y accesos; detectar incompatibilidades de funciones, prevenir conflictos de acceso entre roles; desarrollar una matriz de riesgos de acceso para sistemas críticos como ERP, CRM y HR; y, finalmente, adoptar software de control de accesos que monitoree y prevenga accesos inadecuados.

El control de acceso no solo permite determinar si un usuario tiene los permisos adecuados, sino que también facilita la auditoría de accesos, lo cual es clave para la seguridad financiera y operativa.

Aunque no existe un método 100% infalible para proteger a una organización, la implementación de controles internos sólidos y revisiones constantes reducen significativamente el riesgo de fraude. El uso de marcos regulatorios y software adecuado puede minimizar los impactos de posibles infracciones y asegurar la protección de la información crítica. Ante esto, avanzar hacia una estrategia de control de accesos debe ser una prioridad hoy para las empresas. **/ChN**