Media Contact:
Ken Kadet, VP, Public Relations
952-937-1154 | ken.kadet@entrust.com

Las empresas priorizan la protección de los datos de sus clientes, pero continúan dejándolos expuestos — afirma el Estudio Global de Tendencias de Cifrado de Entrust

Llevada a cabo por el Instituto Ponemon, la decimosexta edición del estudio anual recalca cómo la mitad de las organizacione, incluyendo las españolas, han logrado estrategias consistentes de cifrado, así como otras tendencias clave en materia de cifrado y ciberseguridad

MINEÁPOLIS, EE. UU. — 14 de abril de 2021 — Las empresas ven la protección de la información personal de sus clientes como la principal razón para cifrar datos, y aun así declaran que realmente cifran los datos de sus clientes a un nivel mucho menor. Este y otros hallazgos han sido recalcados en el Estudio Global de Tendencias de Cifrado 2021, la decimosexta edición del estudio anual e internacional llevada a cabo por el Instituto Ponemon que informa sobre los retos en materia de ciberseguridad a los que se enfrentan las organizaciones a día de hoy, y cómo y por qué las organizaciones implementan cifrado.

Amenazas y prioridades
Por segundo año consecutivo, los profesionales de tecnologías de la información (TI) clasifican la protección de la información de sus clientes como el principal impulsor para el despliegue de tecnologías de cifrado. La citada gran desconexión se halla en que la información del cliente se establece en quinto lugar en la lista de tipos de información que las empresas realmente cifran, indicando un gran abismo entre las prioridades de una organización y la realidad a la hora de implementar cifrado.

En España un 77% de las organizaciones afirma que la protección de información de sus clientes es el principal impulsor a la hora de cifrar, una de las cifras más altas en comparación con la media global del 54%. No obstante, tan solo un 27% realmente lleva a cabo dicho cifrado, en comparación con un 42% de media global.

Al analizar lo que las empresas participantes en el estudio realmente cifran, los registros financieros (55%), datos relacionados / vinculados a pagos (55%), datos de empleados / RRHH (48%) y la propiedad intelectual (48%) se sitúan todos por encima de la información personal de los clientes (42%).

“La filtración de información personal golpea en el corazón de la relación entre empresas y sus clientes. El cifrado forma parte de los cimientos de la protección de datos, y cuando las organizaciones no priorizan la protección de información personal de sus clientes, aumentan en

riesgo a la empresa así como la pérdida de negocio y su reputación," afirma John Grimm, vicepresidente de estrategia para Entrust.

El cumplimiento normativo — que hasta recientemente se indicaba como la principal razón para cifrar — tiene una sólida pero decreciente influencia sobre el uso de cifrado, perpetuando la tendencia ya identificada en el Estudio Global de Tendencias de Cifrado de 2020. Tanto la protección de datos de clientes (54%), como la protección frente a amenazas específicas e identificadas (50%), y la protección de la propiedad intelectual (49%), se posicionan por encima del cumplimiento normativo, que se encuentra ahora en un 45%.

La complejidad a la hora de gestionar cifrado y claves en 2021
El estudio también destaca tendencias favorables. Por primera vez, la mitad (el 50%) de las organizaciones informan que tienen una estrategia general de cifrado aplicada de forma consistente, mientras el 37% indica una estrategia de cifrado limitada.

Pero este hito pone a su vez en evidencia nuevas brechas, sobre todo en entornos multi-nube. Las herramientas de cifrado se encuentran en abundancia, con las organizaciones encuestadas informando que usan una media de ocho productos distintos para desempeñar cifrado. Los encuestados también indican que las características más importantes en las soluciones de cifrado son el desempeño, gestión de claves de cifrado, aplicación de políticas y apoyo para tanto la nube y el despliegue en establecimientos. De hecho, el 45% de encuestados califica como muy importantes o de importancia la gestión de claves unificada en tanto múltiples nubes como entornos de empresa. Este hallazgo se encuentra en línea con la afirmación que las claves de cifrado para servicios en la nube — incluyendo Bring Your Own Key (BYOK) — son el mayor reto a la hora gestionar todo tipo de claves, según el estudio.

No sólo es la gestión de claves cada vez más compleja, sino simplemente saber dónde se alojan los datos de la organización en las propias instalaciones, de forma virtual, en la nube o entornos híbridos es un problema contínuo. Como tal, un 65% de organizaciones informa que descubrir dónde se alojan sus datos de carácter sensible continúa siendo, de lejos, el principal reto a la hora de planear y ejecutar una estrategia de cifrado metódica.

El papel cada vez más importante de los módulos de seguridad de hardware (HSMs)
La generación y gestión de claves de cifrado puede ser gestionada de forma más eficiente con el uso de módulos de seguridad de hardware (HSMs). Y la adopción de los mismos está incrementando con dos tercios de todos los encuestados (66%) citando los HSMs como fundamentales para el cifrado o para sus estrategias de gestión de claves, con un crecimiento proyectado que alcanzará el 77% en los próximos 12 meses. El estudio también muestra que, por encima de las aplicaciones tradicionales como por ejemplo TLS/SSL, cifrado de aplicaciones y PKI, los HSMs son implementados cada vez más para casos de uso modernos como cifrado de contenedores / servicios de firma, cifrado de nubes públicas, gestión de secretos y gestión de acceso privilegiado.

A medida que las organizaciones continúan con sus transformaciones digitales, los HSMs juegan un papel cada vez más importante en el entorno de la nube. El estudio revela que el cifrado o servicios de firma para contenedores (40%) son el caso de uso más popular para los HSMs tras el cifrado de aplicaciones (47%) y TLS/SSL (44%). Cifrado de la nube pública, incluyendo BYOK, es el cuarto caso de uso de mayor popularidad para HSM (34%). De particular interés es el uso de los HSMs con soluciones de gestión de secretos, los cuales han subido hasta ocupar el séptimo puesto en la lista de principales casos de uso para los HSM, con un crecimiento estimado de un 5% en los próximos 12 meses.

Blockchain, quantum y la adopción de nuevas tecnologías de cifrado
La percepción sobre nuevas tecnologías de cifrado como la computación multipartita y el cifrado homomórfico es que estas están por lo menos a cinco años vista de ser usadas de forma convencional, según los encuestados. De manera similar, mientras que no se espera que los algoritmos cuánticos sean una consideración seria hasta dentro de ocho años, esta previsión ha acelerado en medio año con respecto a la predicción del mismo estudio en 2020.

Blockchain está más cerca del uso convencional como una tecnología de cifrado. Usado en la actualidad como base de la criptomoneda, se espera que en menos de tres años la adopción de blockchain y sus casos de uso se extiendan hasta incluir:

- Criptomoneda/carteras (59%)
- Transacción/gestión de activos (52%)
- Identidad (45%)
- Cadena de suministro (37%)
- Contratos intelligentes (35%)

“Observando los resultados del Estudio Global de Tendencias de Cifrado 2021 de Entrust, y en el contexto de los últimos 16 años, se muestra claramente que la ciberseguridad y la protección de datos nunca han sido tan complejos, en un momento en el que hay muchísimo en juego,” afirma el Doctor Larry Ponemon, presidente y fundador del Instituto Ponemon. “De manera más pertinente, es alentador que la protección de datos de los consumidores sea una prioridad tan alta para las organizaciones, pero claramente hay trabajo que hacer para convertir esa prioridad en una realidad en cuestión de qué datos son cifrados realmente y en qué puntos del ciclo vital de los mismos. También es aparente que las organizaciones, independientemente de su formación o tamaño, están buscando adoptar soluciones de cifrado para una gama de nuevos e innovadores casos de uso, los cuales sin duda continuarán impulsando la innovación en la industria.”

“TI tiene la tarea de implementar, hacer seguimiento y gestionar el cifrado y políticas de seguridad en las propias instalaciones, en la nube, entornos multi-nube e híbridos, para hacer frente a un creciente despliegue de casos de uso, y en el contexto de crecientes amenazas. El cifrado es esencial para proteger los datos de la empresa y del cliente, pero gestionar el cifrado y proteger las claves de secretos asociados a ellas son cuestiones de creciente dificultad a medida que las organizaciones desarrollan funciones críticas en servicios de múltiples nubes,”

añade Grimm. “El creciente uso de los HSMs para el cifrado y la gestión de claves muestra que las TI están empezando a hacer frente a estos retos. Las organizaciones se beneficiarán de un ecosistema de soluciones integradas para la gestión de políticas de seguridad en la nube, gestión de secretos y manteniendo seguros contenedores, así como el desarrollo de aplicaciones para ayudarles a poner el foco sobre crypto y tenerlo bajo control.”

Algunas de las tendencias clave a nivel global incluyen:

- De los países encuestados, EE. UU. lidera el uso de cifrado (70%, cifra que supera en un 20% la media global) y de los HSMs (72%, que supone un 23% más que la media global).
- Reino Unido cifra la información de sus clientes con un mayor índice (59% en comparación al 42% de media global).
- Suecia registra el mayor uso de cifrado en dispositivos IoT (un 47% lo implementa extensivamente en comparación con un 33% de media a nivel global).
- A pesar de situarse la media global en un 54%, España, Japón y Hong Kong registran la protección de información de sus clientes como el principal impulsor a la hora de cifrar en un 77%, 74% y 72%, respectivamente.
- Los encuestados en Corea están planeando un gran incremento en el uso de HSMs con la aplicación de cifrado en los próximos 12 meses — creciendo de un 40% a un 61%.

Información adicional:
Informe en español: Estudio Global de Tendencias de Cifrado 2021
Blog: https://blog.entrust.com/2021/04/how-do-you-solve-a-problem-like-customer-data-protection

Sobre Entrust Corporation

Entrust mantiene el mundo moviéndose de forma segura al posibilitar identidades, pagos y protección de datos seguros. Hoy más que nunca, las personas demandan experiencias ininterrumpidas y seguras, ya sea cruzando fronteras, realizando una compra, accediendo a servicios electrónicos del gobierno o ingresando en una red corporativa. En el centro de todas estas interacciones Entrust ofrece una amplitud de soluciones sin rival en seguridad digital y emisión de credenciales. Con más de 2.500 compañeros, una red de socios globales y clientes en más de 150 países, no es sorpresa que las organizaciones con mayor confianza del mundo confíen a su vez en nosotros. Para más información visite www.entrust.com.