IoT, autenticación y servicios en la nube impulsan un importante incremento en la adopción de PKI y en el volumen de certificados - revela el nuevo estudio de Entrust

El estudio anual de tendencias en PKI e IoT halla en 2020 niveles sin precedentes de retos en PKI, cambios e incertidumbre

CIUDAD DE MÉXICO – 13 de octubre 2020 – Las organizaciones están aumentando rápidamente el tamaño, alcance y escala de su infraestructura de protección de datos, lo cual queda reflejado en la dramática subida en la adopción de Infraestructura de Clave Pública (PKI por sus siglas en inglés) en empresas en todo el mundo, según el nuevo estudio de Entrust. PKI se encuentra en el núcleo de casi toda infraestructura de tecnología de la información (IT), permitiendo la seguridad para iniciativas críticas digitales como la nube, el despliegue de dispositivos móviles, la identidad y el internet de las cosas (IoT).

El Estudio de Tendencias Globales en PKI e IoT en 2020, llevada a cabo anualmente por la agencia de investigación el Instituto Ponemon y patrocinado por nCipher Security (una compañía de Entrust), se basa en las respuestas de más de 1.900 profesionales de seguridad en IT en 17 países, incluyendo México.

IoT, autenticación y la nube: principales impulsores del incremento en la adopción de PKI
A medida que las organizaciones se tornan más dependientes de la información digital y se enfrentan a cada vez mayores y más sofisticados ciberataques, también dependerán de PKI para controlar el acceso a sus datos y verificar a gran escala las identidades de las personas, sistemas y dispositivos.

IoT es la tendencia de mayor crecimiento que impulsa el despliegue y aplicación de PKI, aumentando un 26 por ciento en los últimos cinco años hasta alcanzar un 47 por ciento en 2020. Los servicios alojados en la nube son el segundo impulsor, citado por el 44 por ciento de los encuestados. En México los encuestados citan IoT como la tendencia más importante (52 por ciento) y también que dependen de proveedores de servicios externos para la dotación de personal PKI más que cualquier otro país (25 por ciento en comparación con la media global del 14 por ciento).

El uso de PKI aumenta para los casos de uso en la nube y para la autenticación
Los certificados TLS/SSL para páginas web y servicios dirigidos al público son citados con mayor frecuencia como los casos de uso para las credenciales PKI (un 84 por ciento de encuestados). Las aplicaciones públicas alojadas en la nube experimentaron el mayor crecimiento en comparación con el año anterior, citado por un 82 por ciento (lo cual supone un aumento del 27 por ciento con respecto a la cifra en 2019), seguido por la autenticación de usuarios de empresa, indicada por un 70 de los encuestados (lo cual supone un incremento del 19 por ciento en comparación con la cifra en 2019). Todos subrayan la necesidad crítica de implementar PKI para apoyar las aplicaciones centrales del negocio.

La media del número de certificados que una organización necesita gestionar creció un 43 por ciento en el estudio de 2020 en comparación con el año anterior, de 39.197 a 56.192 certificados, lo cual recalca un requisito fundamental para la gestión de certificados de empresa. Es probable que este incremento esté motivado por la transición de la industria a periodos más cortos de validez de

certificados, y un incremento agudo en el número de casos de uso ligados a la autenticación de usuarios en la nube y en la empresa.

Retos, cambio e incertidumbre
El estudio de 2020 halla que los profesionales de IT están haciendo frente a nuevos retos a la hora de habilitar aplicaciones para que usen PKI. Más de la mitad (un 52 por ciento) cita como reto principal la falta de visibilidad de las capacidades de seguridad de una PKI ya existente, lo cual supone un incremento del 16 por ciento en comparación con el estudio de 2019. Esta cuestión subraya la falta de experiencia en materia de ciberseguridad existente incluso dentro de las organizaciones con mejores recursos, así como la necesidad de especialistas en PKI que puedan crear hojas de ruta empresariales, customizadas en base a buenas prácticas de seguridad y operacionales. Los encuestados también citan como retos cruciales la incapacidad de cambiar aplicaciones heredadas y la incapacidad de las PKI ya existentes de respaldar nuevas aplicaciones – ambos en un 51 por ciento.

A la hora de implementar y gestionar PKI, los profesionales de seguridad en IT se encuentran más retados por asuntos organizacionales tales como la falta de responsabilización, así como insuficientes habilidades y recursos. Las cifras del estudio relativas al despliegue de PKI indican claramente una tendencia hacia enfoques más diversificados, incluso llegando a convertirse en algunos países en más prevalentes las ofertas 'como servicio' que en las mismas instalaciones. En México, un 81 por ciento de encuestados declara que el principal reto a la hora de implementar y gestionar PKI era la clara falta de responsabilización.

Las dos áreas de mayor cambio e incertidumbre en PKI derivan de nuevas aplicaciones como IoT (citado por el 52 por ciento de los encuestados) y los mandatos y estándares externos (un 49 por ciento). El ambiente reglamentario también está impulsando de manera creciente el despliegue de aplicaciones que usen PKI, indicado por un 24 por ciento de los encuestados. Un 59 por ciento de los encuestados mexicanos citan los mandatos y estándares externos como las áreas de mayor cambio e incertidumbre en la evolución de PKI.

Las prácticas de seguridad no han seguido el ritmo del crecimiento
En los próximos dos años, un promedio del 41 por ciento de dispositivos IoT dependerán primordialmente de certificados digitales para su identificación y autenticación. A pesar de aumentar el cifrado de dispositivos IoT, plataformas y repositorios de datos, este tan sólo se sitúa en un 33 por ciento – suponiendo un posible punto de exposición al público de datos de carácter sensible. Los encuestados citan varias amenazas a la seguridad IoT, incluyendo la alteración de la función de los dispositivos IoT a través de malware u otros ataques (68 por ciento) y el control remoto del dispositivo por un usuario no autorizado (54 por ciento). Sin embargo, los encuestados clasifican los controles relativos a la protección ante posible malware – como la emisión segura de parches y actualizaciones para dispositivos IoT – en último lugar en su lista de cinco funciones de seguridad IoT más importantes.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) recomienda que los módulos criptográficos para las autoridades de certificación (CAs), los servidores de recuperación de claves y respondedores del protocolo de estado de certificado en línea (OCSP) sean validados en base al estándar FIPS 140-2 de nivel 3 o mayor. El 39 por ciento de los encuestados para este estudio usa Módulos de Seguridad de Hardware (HSM por sus siglas en inglés) para mantener

seguras su PKI, en la mayoría de los casos para gestionar sus claves privadas para sus CA de raíz, emisión o reglamento. Sin embargo, sólo un 12 por ciento de encuestados indica que usa HSM en sus instalaciones OSCP, lo cual pone en evidencia una brecha significativa entre buenas prácticas y prácticas observadas.

En México el uso de controles de PKI y buenas prácticas tiende a estar por debajo de la media, particularmente el uso de una ubicación segura citado por un 31 por ciento de encuestados en el país frente al 49 por ciento global. Adicionalmente, México se sitúa en el tercer puesto a nivel global a la hora de usar autoridades internas de certificación corporativa (79 por ciento).

“PKI apoya la seguridad de tanto el mundo de negocios como la del consumidor, englobando desde la firma digital de transacciones y aplicaciones para probar la fuente tanto como la integridad, hasta el apoyo en la autenticación de smartphones, videoconsolas, pasaportes de ciudadanos, sistema de tickets para el transporte público y la banca móvil,” afirma Larry Ponemon, fundador del Instituto Ponemon. “El Estudio de Tendencias Globales en PKI e IoT en 2020 nos muestra un aumento en el uso de credenciales de PKI para aplicaciones en la nube y la autenticación de usuarios de empresa, recalcando el papel crítico que desempeña PKI en apoyar las aplicaciones fundamentales de negocio.”

“Estamos viendo un incremento en la dependencia de PKI, yuxtapuesto con la lucha de equipos internos por adaptarlo a los nuevos mercados y sus necesidades – impulsando cambios en los modelos de despliegue y métodos tradicionales de PKI,” dice John Grimm, vicepresidente de estrategia para soluciones digitales de Entrust. “En sectores más nuevos como lo es IoT, las empresas claramente están fracasando a la hora de priorizar mecanismos de seguridad como la firma de firmware que contrarresten las amenazas más urgentes, como el malware. Asimismo, con el incremento masivo de certificados emitidos y adquiridos que fueron identificados en el estudio de este año, la importancia de implementar una gestión automatizada de certificados, un enfoque flexible de despliegue de PKI y una seguridad robusta basada en buenas prácticas incluyendo HSM, nunca ha sido mayor.”

Descargue su copia del nuevo Estudio de Tendencias Globales en PKI e IoT en 2020.

Metodología del Estudio de Tendencias Globales en PKI e IoT en 2020
El *Estudio de Tendencias Globales en PKI e IoT en 2020* capta el estado actual de madurez de la infraestructura de clave pública (PKI por sus siglas en inglés), sus retos y la influencia del Internet de las Cosas (IoT) sobre sus tendencias. El estudio recoge los resultados de la quinta encuesta anual completada por 1.934 profesionales de tecnología de la información en los siguientes 17 países / regiones: Australia, Brasil, Francia, Alemania, Hong Kong, India, Japón, México, Oriente Medio (Arabia Saudita y los Emiratos Árabes), Países Bajos, Federación Rusa, Corea del Sur, Sudeste Asiático (Indonesia, Malasia, Filipinas, Tailandia y Vietnam), Suecia, Taiwán, Reino Unido y los Estados Unidos.

El estudio de 2020 es la quinta encuesta anual sobre tendencias globales en PKI e IoT, patrocinado por nCipher Security (una compañía de Entrust) y líder en el mercado de los Módulos de Seguridad de Hardware (HSMs) de uso general, los cuales empoderan a las organizaciones líderes en el mundo

al brindarles confianza, integridad y control sobre su información y aplicaciones críticas empresariales.

Acerca de Entrust
Entrust mantiene el mundo moviéndose de forma segura al posibilitar identidades, pagos y protección de datos. Hoy más que nunca, la gente demanda 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 saber más visite www.entrust.com.

###

Para más información por favor contacte:

Liz Harris liz.harris@ncipher.com +44 7973 973648
Ken Kadet ken.kadet@entrust.com +1 952-988-1154