Publicado en Boston y Londres el 20/06/2023

GlobalSign aconseja a las empresas que se preparen para cambios en PKI que empezarán en otoño hasta 2024

Una autoridad de certificación líder alerta a las industrias sobre los próximos avances en ciberseguridad en un mercado en el que confían millones de organizaciones de todo el mundo

A finales de este año y en 2024, se producirán cambios significativos en el mercado de la infraestructura de clave pública (PKI) y las organizaciones de todo tipo deben ser conscientes de estos cambios, según GMO GlobalSign, Inc. una autoridad de certificación (CA) global y proveedor líder de soluciones de seguridad de identidad, firma digital e IoT: La medida de Google para reducir la vida útil de los certificados SSL/TLS, los nuevos requisitos básicos del Foro CA/Browser para la seguridad del correo electrónico y los cambios Root obligatorios emitidos por Mozilla. Los próximos cambios tendrán un impacto significativo en las industrias que utilizan PKI, en las que confían millones de empresas de todo el mundo. Estos cambios exigirán que las empresas adapten su PKI para garantizar el cumplimiento continuo de la seguridad.

Transición a certificados SSL/TLS de 90 días

Las organizaciones que dependen de PKI deben estar informadas del anuncio de Google del 3 de marzo, en el que propone un límite máximo obligatorio de validez de 90 días para los certificados SSL/TLS. El ciclo de vida actual de los certificados SSL/TLS es de 398 días. Se recomienda encarecidamente a las empresas que evalúen ya sus procesos de ciclo de vida de los certificados y estén preparadas para estos cambios a fin de seguir siendo seguras. Esta evolución puede obligar a las empresas a reestructurar su infraestructura informática y a disponer de nuevas tecnologías, en concreto de automatización, para garantizar una gestión continuada del ciclo de vida de los certificados.

"Los administradores de sitios web tendrán que pasar a la automatización si/cuando entre en vigor el plazo máximo de validez de certificados y reutilización de dominios de 90 días propuesto por Google. Cada vez va a ser más difícil sustituir los certificados mediante CSR generados manualmente e instalaciones posteriores de certificados a medida que se acorten los periodos de validez y revalidación de dominios", afirma Doug Beattie, Vicepresidente de Gestión de Productos de GlobalSign. "Tecnologías como la oferta ACME de GlobalSign ayudan a automatizar las funciones del ciclo de vida de los certificados y garantizan que los certificados se sustituyen automáticamente mediante procesos totalmente automatizados antes de que caduquen. Esto mantiene a las empresas seguras y evita que sus sitios web utilicen certificados caducados, lo que se traduce en pérdidas de negocio".

Cambios en los requisitos básicos de S/MIME

En enero, el CA/B Forum, un consorcio de fabricantes de navegadores, autoridades de certificación y otras organizaciones del ecosistema de certificados digitales, acordó un nuevo conjunto de normas denominadas "Requisitos básicos para la emisión y gestión de certificados S/MIME de confianza pública" para establecer los requisitos detallados del sector para los certificados S/MIME. Las nuevas

normas suponen un cambio que entrará en vigor el 1 de septiembre. Esto significará perfiles de certificado estandarizados que requerirán una validación organizativa o individual adicional y, en algunos casos, las CA tendrán que sustituir sus CA S/MIME actuales por otras nuevas y conformes. Disponer de una norma industrial para los certificados S/MIME mejora la interoperabilidad y la seguridad y es paralelo a lo que se ha hecho para los certificados TLS y Code Signing.

Mozilla planea desconfiar de los certificados raíz antiguos

Mozilla ha anunciado planes para eliminar los bits de confianza SSL/TLS y S/MIME en las Roots cuando cumplan 15 y 18 años respectivamente. La medida se toma porque algunas de las Root más antiguas no cumplen los requisitos actuales de las Root y para promover la agilidad criptográfica. Los bits de confianza SSL/TLS de las Root R1 y R3 de GlobalSign se eliminarán en abril de 2025 y abril de 2027, respectivamente. "Como resultado, dejaremos de emitir certificados SSL/TLS bajo estas Roots en 2024 y 2026. A finales de este año se publicarán más detalles sobre los planes de GlobalSign".

Experiencia, conocimientos y fiabilidad

Con 27 años de experiencia, GlobalSign es su fuente fiable de recomendaciones, independientemente del tamaño de la organización, sobre la mejor forma de afrontar estos importantes cambios del sector. Dado que las empresas que utilizan PKI no tienen elección en los cambios que se están realizando en los certificados públicos, es fundamental que las empresas ajusten su postura de seguridad y automatización de PKI lo antes posible para seguir siendo resistentes.

Beattie añadió: "Comprendemos las preocupaciones que generan estos cambios, especialmente entre las empresas más pequeñas. Pero hay un lado positivo: En GlobalSign, estamos preparados para acompañar a cada cliente paso a paso en este viaje y pueden estar seguros de que les equiparemos con los métodos y servicios necesarios, ya sean empresas, PYMES o proveedores de servicios. De esta forma, todas las empresas podrán operar en el futuro de forma similar a como lo hacen hoy, sin que el impacto de estos cambios sea tan drástico".

https://www.globalsign.com.

Datos de contacto:
Amy Krigman
Director of Public Relations, West Region

Nota de prensa publicada en: Boston y Londres

Categorías: Internacional Finanzas Software Ciberseguridad