White Paper

Según un estudio reciente, las inversiones en PKI ayudan a que las organizaciones mejoren la seguridad y modernicen los procesos comerciales

Patrocinado por: DigiCert Inc.

Robert Westervelt
August 2019

RESUMEN EJECUTIVO

Los equipos de operaciones y los profesionales de seguridad de TI están bajo una presión cada vez mayor para administrar la seguridad y la resiliencia de sistemas de misión crítica que brindan soporte a iniciativas de transformación digital (DX) empresarial de rápida evolución. En una apuesta que intenta aliviar la presión y asignar recursos con mayor eficiencia en los entornos multinube e híbridos cada vez más comunes, los directores de información, los directores de seguridad de la información (CISO) y los arquitectos de seguridad ahora están revisando las implementaciones de infraestructura de clave pública (PKI) que frecuentemente son inconexas y están mal administradas.

La PKI es la columna vertebral de muchas organizaciones que valoran la resiliencia de ciberseguridad, ya que les permite automatizar el proceso de aplicar políticas y procedimientos de seguridad de datos con certificados digitales y cifrado de claves públicas. La PKI fue diseñada para establecer conexiones validadas y de confianza entre sistemas, y para ofrecer acceso de usuario sin restricciones a recursos sensibles. Con el paso del tiempo, la PKI creció y pasó a proteger documentos, correos electrónicos e integridad de código mediante certificados con firma criptográfica. Además, se encargó de proteger activos e individuos con identidades digitales mediante certificados de dispositivos.

En la actualidad, cuando los equipos de seguridad están bajo la mayor presión de la historia, la PKI se somete a pruebas exhaustivas y se utiliza de manera generalizada como sistema confiable. Los equipos usan PKI para remediar riesgos a medida que el negocio usa más servicios de nube. Por su parte, los atacantes aprovechan las complejidades y los problemas de configuración provocados por una infraestructura de seguridad fragmentada. Para los CISO, enfrentar este desafío es una prioridad, según la *Encuesta de servicios de datos para nube híbrida* de IDC, que alcanzó a más de 400 especialistas en administración de datos y seguridad de TI en Europa y América del Norte. En la encuesta, aproximadamente el 65 % de las organizaciones informaron el uso de certificados digitales y PKI para brindar soporte a distintas funciones, entre ellas:

- **BYOD seguro:** para brindar soporte a iniciativas de BYOD no controladas y mantener un acceso seguro a los recursos de la empresa sin sacrificar la experiencia del usuario móvil
- **Autenticación segura:** para autenticar individuos de manera sólida en aplicaciones que contienen información sensible

- **Acceso remoto seguro:** para autenticar empleados y partners de manera sólida en una red inalámbrica o una VPN para acceso seguro
- **Correo electrónico seguro:** para permitir que los usuarios de correo electrónico envíen mensajes cifrados y con firma digital a través de todos los dispositivos corporativos
- **Integridad de firma de documentos:** Para validar la integridad y la autenticidad de las firmas digitales en documentos críticos
- **Dispositivos de la Internet de las cosas (IoT) seguros:** para ofrecer identidad de dispositivos, establecer una raíz de confianza y mantener la integridad de software y firmware en dispositivos de la IoT sensibles

A medida que las organizaciones siguen usando PKI para la seguridad en distintos frentes, y los atacantes siguen sofisticándose y mejorando la frecuencia contra datos sensibles, los equipos de seguridad deben implementar enfoques más integrales y coordinados para brindar soporte a estrategias comerciales en permanente evolución. IDC estima que el 60 % de las organizaciones tendrán una estrategia de transformación digital en curso en los próximos 24 meses. La transformación de TI (ITX) es un componente clave de una estrategia DX. Por su parte, la seguridad y la disponibilidad de datos son pilares de la ITX. La PKI cumple un rol fundamental para mantener la integridad, la disponibilidad y la resiliencia de la infraestructura de TI de una organización. Pero administrar la protección de datos entre estos entornos cada vez más híbridos tiene una complejidad creciente, en un contexto donde las amenazas son muy diversas y sofisticadas. La última serie de violaciones de datos de alto perfil ilustra los problemas creados por los entornos corporativos altamente distribuidos e intrincados que existen actualmente. Los atacantes aprovechan los costosos errores que dejan los servidores de datos abiertos a la Internet pública. Siguen explotando contraseñas débiles, predeterminadas o robadas, y están sondeando constantemente vulnerabilidades creadas por la administración de datos en entornos distribuidos. Más del 30 % de los encuestados citaron la dificultad de integrar sus entornos híbridos y multinube con la infraestructura de TI existente, mientras que el 37 % mencionó a la complejidad de las soluciones de TI como una de las tres principales amenazas que enfrentará su organización en los próximos dos años (el primer y el segundo lugar fueron la mayor sofisticación de los atacantes y los riesgos de adopción de la nube). Con frecuencia, el problema está compuesto por operaciones de PKI dañadas que pueden inhibir la productividad del usuario, erosionar la confianza entre clientes y partners, y provocar costosos incidentes de seguridad y violaciones de datos.

El soporte de PKI para aplicaciones de negocios críticas es "altamente efectivo"

Las entrevistas realizadas para este estudio transmitieron una impresión ampliamente positiva sobre la manera en que la PKI puede integrarse de forma transparente con distintas aplicaciones de negocios empresariales específicas de la industria. Las implementaciones de PKI recibieron elogios por escalar al manejo de aplicaciones de pagos complejas y terminales de punto de venta (POS) de acceso remoto y por su capacidad de integración con distintos sistemas backend, entre ellos repositorios de análisis avanzados que brindan soporte para cifrado, y también por permitir la firma de documentos digitales con el fin de mantener la integridad de los contratos en el campo a través de un sistema de administración de contenidos personalizado.

Los CISO y los arquitectos de seguridad expresaron opiniones abrumadoramente positivas acerca de la PKI. La calificaron como "altamente efectiva" cuando la tecnología se implementa y se administra de forma proactiva. La mayoría de los entrevistados están trabajando con varias implementaciones de PKI integradas con aplicaciones de negocios empresariales específicas de la industria y Active

Directory. Han administrado o supervisado la administración de PKI durante un tiempo considerable, que les permitió experimentar el crecimiento y el cambio en sus organizaciones. Además, han trabajado con varias actualizaciones a sus implementaciones de PKI existentes para mantener una posición de seguridad sólida. IDC recomienda que las organizaciones de TI tomen estas medidas para reforzar la efectividad de la PKI:

- Identificar si la organización puede atraer, capacitar y retener arquitectos de seguridad para administrar las implementaciones de PKI existentes, y determinar si el equipo tiene la experiencia para brindar soporte a nuevos objetivos comerciales que requieren la aplicación ampliable de certificados digitales.
- Considerar el aprovechamiento de servicios de PKI administrados para optimizar la gestión y reducir la complejidad. Una vez que las operaciones de PKI están diseñadas e implementadas, cambiar las especificaciones y los procesos puede ser engorroso. La inversión inicial es crucial.

METODOLOGÍA

Para este estudio de IDC, se entrevistó a directores de seguridad de la información y arquitectos de seguridad en varias empresas importantes. Se les consultó sobre su infraestructura de PKI existente y la forma en que se adaptó para brindar soporte a las estrategias de adopción de la nube y la transformación digital en sus organizaciones. Los conocimientos adquiridos en estas entrevistas se combinaron con nuevos datos de estudios relacionados con los desafíos de proteger entornos híbridos y multinube. El estudio identificó eficiencias mejoradas y menores costos de administración relacionados con una variedad de casos de uso, entre ellos implementaciones de PKI administradas e in situ que brindan soporte para la firma de código con el fin de validar la autenticidad de actualizaciones de software en dispositivos de la IoT, firma de documentos para eliminar procesos manuales y en papel, correo electrónico seguro, acceso remoto seguro, y autenticación de usuarios y máquinas relacionada con recursos sensibles de la compañía.

DESCRIPCIÓN GENERAL DE LA SITUACIÓN

Aspectos esenciales de PKI para evitar ataques exitosos y proteger recursos críticos

Muchas organizaciones están buscando ayuda de especialistas en PKI para optimizar, centralizar y automatizar la administración de certificados digitales como parte de iniciativas de transformación digital para eliminar infraestructura fragmentada y redundante y reducir costos. Esta ayuda incluye automatizar la administración de una o varias implementaciones de PKI para brindar soporte a distintas unidades de negocios a un servicio de PKI administrado para asegurar un mantenimiento confiable y proactivo.

Este estudio descubrió que las reducciones de costos y las mejoras de eficiencia se citan frecuentemente como motivos detrás de las inversiones en PKI. Sin embargo, los principales impulsores de las implementaciones de PKI son las debilidades y las vulnerabilidades que surgen de la complejidad de implementar y administrar productos de seguridad. Casi el 40 % de los especialistas en seguridad de TI, línea de negocios y administración de datos citaron la creciente sofisticación de los ataques y la mayor complejidad de administrar y brindar soporte como desafíos significativos, según la *Encuesta de servicios de datos para nubes híbridas* de IDC. La investigación de IDC ha

demostrado que los equipos de seguridad enfrentan problemas de seguridad y privacidad cada vez mayores. Están sometidos a una presión cada vez mayor de cumplir y mantener una cantidad de obligaciones de cumplimiento en permanente crecimiento, y deben defenderse constantemente contra el crecimiento de los ciberataques de varios frentes y dirigidos contra recursos corporativos críticos.

Además de los daños de reputación, los costos directos y las sanciones regulatorias mencionadas anteriormente, los ciberataques pueden provocar tiempo improductivo no planificado, pérdida de secretos comerciales competitivos y pérdida de datos permanente. La investigación de IDC ha demostrado que el costo promedio de los tiempos improductivos en la industria es de USD 250 000 por hora. La comparación de los costos de prevención de ataques y del software de recuperación con apenas una hora de tiempo improductivo justifica el costo. En muchos casos, ahora las violaciones de seguridad requieren una divulgación pública, una garantía casi segura de daños ala reputación que frecuentemente dura mucho tiempo, sin manera de recuperar los datos o los clientes perdidos de forma permanente. La investigación de IDC ha revelado que se producen daños a la reputación en casi la mitad de las situaciones de violaciones de datos, algo que aumenta aún más los costos de recuperación y reparación.

Las violaciones de seguridad, que cobran un estado cada vez más público, son un recordatorio constante para empresas y consumidores de que las credenciales de identidad son el corazón mismo de la seguridad. Innumerables estudios han demostrado que los problemas de vulnerabilidad y configuración, que a menudo son consecuencias de la mayor complejidad, contribuyen a los incidentes de seguridad. La reducción de las implementaciones de PKI fragmentadas e inconexas puede ayudar a reducir los errores del usuario y del sistema que son aprovechados por los atacantes, y también a evitar la fuga de datos en el proceso. La PKI, si se implementa y se administra adecuadamente, es una de las herramientas más potentes que pueden usar las organizaciones para evitar violaciones de datos costosas y perjudiciales para la imagen. Una cantidad cada vez mayor de organizaciones están revisando sus estrategias de cifrado y administración de claves para tener una mayor conciencia de la situación y, a su vez, mejorar sus posiciones de seguridad.

Los profesionales de seguridad entrevistados para este estudio consideraron que la PKI era un componente esencial y comprobado para brindar soporte al cifrado de datos y validar la integridad de datos y transacciones. Además, afirmaron que es crítico para verificar las identidades de usuarios y máquinas en sus organizaciones. La PKI puede subir la barrera que debe superar un atacante para acceder a recursos críticos. Además, la PKI brinda soporte para la seguridad ampliable requerida para importantes procesos comerciales de alta velocidad o en varios frentes, y ha demostrado mejorar la productividad de usuarios y la retención de clientes gracias a su transparencia para las actividades del usuario final.

Un tema que surgió en las entrevistas es la batalla permanente entre la aplicación de seguridad y los usuarios finales que suelen frustrarse con las medidas de seguridad. En respuesta, los practicantes de seguridad están recurriendo cada vez más a proveedores de PKI para diseñar soluciones que funcionen de manera confiable con la infraestructura de TI y seguridad existente una vez identificados los riesgos de un emprendimiento comercial. Para las organizaciones que optan por diseñar y administrar de forma proactiva una solución de PKI, la seguridad es el factor clave para lograr funcionalidad o productividad. Si se implementa adecuadamente, la PKI moderna puede reducir la cantidad de pasos que deben seguir los usuarios finales para completar tareas que requieren autenticación. Los procesos de seguridad que solían ser costosos y crear roces entre usuarios comerciales, ahora pueden automatizarse en gran medida. Las consideraciones de seguridad suelen ser fundamentales luego de las conclusiones de una auditoría, una violación de datos, un incidente de seguridad o, como suele suceder, para satisfacer ciertos requisitos de

cumplimientos regulatorios o políticas de la compañía. En la actualidad, las organizaciones suman capacidades a las que la PKI brinda soporte, como la autenticación de varios pasos, el cifrado y la conectividad móvil.

Algunos CISO entrevistados para este estudio fueron presionados por el CIO para reducir costos y admitir iniciativas de prioridad de la nube, con presupuesto para evaluar el estado de su infraestructura de PKI. Identificaron y documentaron implementaciones de PKI que comenzaron a ceder ante la misma presión provocada por la adopción tecnológica y el crecimiento comercial a gran velocidad. En algunas situaciones, la infraestructura existente en estas organizaciones no tenía un buen mantenimiento debido a la incapacidad para atraer y conservar especialistas en seguridad de TI talentosos. Algunas organizaciones mantenían implementaciones de PKI fragmentadas debido a fusiones y adquisiciones de unidades de negocios individuales que demandaban entornos por separado a causa de restricciones de seguridad o de procesos. Los desafíos de complejidad casi siempre consisten en la naturaleza creciente y distribuida de los recursos de los entornos corporativos. La *Encuesta de servicios de datos para la nube híbrida* de IDC indica que las organizaciones siguen combatiendo estos problemas. Se citó a la PKI como un gran desafío para las organizaciones, igual de complejo que la implementación y la administración de cifrado o la implementación y el ajuste de plataformas para prevenir la pérdida de datos.

CASOS DE USO DE PKI

Los casos de estudio incluidos en las secciones a continuación ponen de manifiesto la manera en que las organizaciones están impulsando la PKI para satisfacer sus requisitos específicos.

La PKI para seguridad de correo electrónico y autenticación mejora la posición de seguridad de un fabricante

Para este fabricante de productos de consumo global, la ciberseguridad jamás había sido una prioridad importante. La falta de una manera confiable y efectiva de autenticar a los empleados que acceden a recursos sensibles o validan la integridad de empleados remotos que solicitan acceso provocó debilidades graves que la compañía ignoró en gran medida. Un ataque de ransomware disruptivo, que adoptó la forma del malware SamSam, finalmente logró capturar la atención de la gerencia sénior en la compañía principal del fabricante. La inversión en PKI para respaldar la seguridad de correo electrónico y la autenticación de usuarios de este fabricante estuvo entre las primeras medidas tomadas por la gerencia sénior.

Los atacantes detrás del malware SamSam identificaron y explotaron fácilmente una vulnerabilidad asociada con los servidores FTP de la compañía, y desataron un ataque de fuerza bruta contra contraseñas débiles como primer paso. Esta costosa violación forzó a la compañía a interrumpir prácticamente toda la producción, algo que tuvo un costo de millones de dólares por día. Debido a que no había copias de seguridad efectivas, los empleados ayudaron en la recuperación de propiedad intelectual (PI) valiosa en formato de papel. A su vez, parte de la PI se restauró desde una copia de seguridad en cinta. Para mejorar la infraestructura de seguridad, la compañía asumió el compromiso de realizar grandes inversiones, incluido el uso de PKI para proteger el correo electrónico.

"Me contrataron para diseñar un programa de seguridad desde cero. Había políticas vigentes, pero nada más allá de eso", explicó el CISO, que se incorporó a la empresa poco después del ataque para diseñar un programa de seguridad y elevar los estándares al nivel de la compañía principal del fabricante. "Nuestras aplicaciones no estaban actualizadas, y nuestra infraestructura de seguridad complementaria

estaba mal configurada o era inexistente. Una vez que entendimos bien dónde residían los datos sensibles, consideramos necesario implementar las herramientas adecuadas. Por eso, rediseñamos la infraestructura de seguridad con una PKI moderna para autenticación de usuarios y protegimos los correos electrónicos de todos nuestros usuarios, más allá de su ubicación o del dispositivo utilizado".

El equipo de seguridad necesitaba garantizar que los futuros mensajes de correo electrónico y archivos de datos transferidos fueran seguros, y trabajaron junto con la compañía principal para implementar la PKI como parte de la migración de una implementación desactualizada de Lotus Notes a Microsoft Office 365. La compañía comenzó con la autenticación de dos factores y utilizó certificados de clientes para eliminar contraseñas débiles y validad la identidad de las 1300 cuentas de Office 365, integrando PKI con los servicios federados de Microsoft Active Directory.

La compañía habilitó los certificados S/MIME, que pueden usarse de manera predeterminada para brindar soporte de cifrado e integridad, ya que ofrecen servicios de firma digital para empleados, incluida la funcionalidad de solicitar un acuse de recibo al trabajar con otros empleados, partners o colaboradores externos. Un dispositivo de correo electrónico analiza los mensajes entrantes y salientes, y además se implementan proxies web como protección del correo electrónico y la web. Este enfoque mejoró en gran medida la posición de seguridad del fabricante, ya que la incorporación de S/MIME puede prevenir los ataques tipo "man-in-the-middle" (MITM) y ofrecer un beneficio aún mayor al cifrar la propiedad intelectual crítica en los casos necesarios.

Además de invertir en herramientas de seguridad, la compañía sumó iniciativas de capacitación y toma de conciencia. "Si deben manejar contenidos restringidos o altamente restringidos, nuestros empleados saben que deben usar cifrado, aunque se trate de mensajes de correo electrónico internos", afirma el CISO.

La compañía principal del fabricante trabajó junto a un especialista en PKI para diseñar la implementación y ajustarla para no alterar el flujo de mensajes de correo electrónico. Hubo algunos problemas de inscripción y de compatibilidad con políticas de seguridad existentes, que rechazaban o ponían en cuarentena el tráfico cifrado que alteraba la entrega de mensajes. El CISO señaló que, en retrospectiva, debería haberse contemplado una mayor planificación en la administración del programa de capacitación. "Los empleados aceptaron las nuevas políticas y los cambios en los procesos provocados por el incidente de malware", agregó. En la actualidad, la empresa sigue obteniendo ventajas gracias a la maduración de su programa de seguridad.
Lanzó un ejercicio de detección y clasificación de datos, y sigue implementando mejoras en seguridad perimetral para sus activos in situ.

PKI utilizado para proteger la experiencia de préstamos moderna e integrado con herramientas de análisis avanzado

Un importante banco, que intenta modernizar sus procedimientos para otorgar préstamos con el fin de mejorar la experiencia del cliente, recurrió a una solución de PKI para proteger sus documentos de préstamo digitalizados y garantizar que los documentos permanecieran cifrados, de acuerdo con las obligaciones de cumplimiento. La seguridad fue una parte significativa de la inversión, y no puede ser un obstáculo para el objetivo general de crear una experiencia dinámica y optimizada con nuevos clientes.

El banco evaluó las soluciones de seguridad que podrían potencial la estrategia comercial de acelerar sus procesos de préstamo, desde el origen hasta el cierre. El equipo de evaluación buscó soluciones de PKI que tuvieran la flexibilidad suficiente para implementarse en el campo e integrarse con la

infraestructura de backend existente. La rotación de empleados en algunas áreas requería una solución que no solo fuera fácil de usar, sino que además ocupara poco espacio y tuviera un buen rendimiento pese a su integración con distintas autoridades de certificados.

El banco debía diseñar una solución que pudiera analizar contenido no estructurado en el lago de big data para convertirlo en datos estructurados compatibles con el motor de inteligencia artificial que ejecuta el asistente virtual. El banco tenía los recursos necesarios para invertir en científicos de datos, además de un equipo de desarrollo para asumir esta tarea. Las soluciones de PKI fueron la elección obvia para brindar soporte a la seguridad de estos datos.

Se requería un servicio de PKI para integrarse con el software de cumplimiento interno que supervisa la incorporación de nuevos clientes. Los requisitos de seguridad también demandaban capacidades de recuperación ante desastres sólidas y de alta disponibilidad, y una instancia dedicada del servicio de PKI que funcione dentro de la nube privada del banco. Además, la solución PKI debía brindar soporte para el cifrado de los documentos de préstamo, además de integrarse con el repositorio de contenidos del banco y con un entorno de análisis avanzado que se utiliza fuertemente en la retención de clientes y la mejora de las ofertas de servicios del banco.

"El tiempo improductivo era algo inaceptable, y necesitábamos garantías de que estábamos en control total con las claves de nuestro lado", le dijo el CISO a IDC. "Sabíamos que una PKI era la mejor manera de resolver nuestros requisitos de seguridad relacionados con activos altamente críticos. Hemos observado numerosas mejoras en el lado comercial. Hasta ahora, eso ha inspirado confianza en nuestra capacidad de proteger estas transacciones críticas sin descuidar nuestras obligaciones de cumplimiento".

La implementación requiere un código base en el servidor, y aprovecha a los agentes en terminales para cumplir los requisitos de cifrado y firma digital en la creación y el envío de documentos. Todo el flujo de trabajo se supervisa y se registra en la web a través del protocolo HTTPS. La autoría de documentación está a cargo del empleado en la terminal, pero el repositorio está en el servidor.

El repositorio de contenidos del banco y un entorno de análisis avanzado se integran con un nuevo asistente virtual, diseñado para automatizar el proceso de obtener firmas del prestatario y eliminar las complicaciones del proceso de préstamo. Las solicitudes de préstamos ya no se escanean, imprimen y envían por fax. Una vez que la solución de PKI valida la identidad del prestatario, este ya no necesita visitar una sucursal y sentarse junto a un ejecutivo de cuentas o el gerente de relaciones para finalizar los documentos. Ahora un solicitante puede realizar cada uno de los pasos de forma segura en línea, desde la comodidad de su hogar. Actualmente, la solución tiene la capacidad de escalar para admitir hasta 20 000 personas, incluido personal legal, funcionarios de riesgo y cumplimiento, funcionarios de préstamo, clientes y otras personas involucradas en el proceso de un préstamo.

"La implementación de la solución de PKI requiere una planificación cuidadosa", explica el CISO. "La optimización y la centralización de la infraestructura de seguridad es algo lógico, pero siempre hay obstáculos políticos, entre ellos el riesgo de exponer datos", continúa. "Si se ponen todos los huevos en una canasta, existe la posibilidad de ser víctima de un hackeo. Lo que se debe tener para alcanzar la centralización es una solución de análisis de conducta de usuarios que atraviese todos los silos".

Un banco regional se actualiza e incorpora una solución de PKI administrada para brindar soporte de movilidad y mayor verificación

Un importante banco regional diseñó su programa de PKI durante varios años, administrando la infraestructura para brindar soporte a su autoridad de certificación (CA) interna. Sin embargo, se enfrentó al creciente problema de reclutar profesionales de seguridad talentosos y de capacitarlos y retenerlos para administrar la infraestructura de seguridad. La complejidad de administrar un programa de PKI fragmentado hizo que algunos miembros del equipo de seguridad "huyeran", según un ingeniero en jefe de seguridad del banco que fue entrevistado por IDC.

El equipo de TI interno se esforzó por administrar varias implementaciones de PKI que se encargaban de la autenticación de usuarios. Se habían diseñado soluciones individuales durante el curso de casi diez años para brindar soporte a tarjetas inteligentes, una solución para acceso a VPN y dispositivos móviles, y un sistema paralelo que brindaba soporte al cifrado y la firma de mensajes de correo electrónico. La complejidad de estas soluciones individuales solía alterar la operación de los usuarios finales debido a un mecanismo anticuado de emisión de certificados. La CA interna solía omitir la publicación de nuevas listas de control de acceso, y frecuentemente las personas no podían autenticarse en la red. Había varias razones por las que podía producirse un fallo; a veces se trataba del error de un módulo de seguridad de hardware o del error de un servidor Windows. "Pueden suceder muchas cosas", afirmó un ingeniero de seguridad.

"Temíamos haber llegado a un punto donde potencialmente podíamos provocar un colapso de toda la red. Si ninguno de nuestros usuarios puede acceder a ciertas aplicaciones ni autenticarse cuando no hay acceso a la PKI, colocaríamos a nuestro equipo en una situación muy incómoda", le dijo el ingeniero de seguridad a IDC.

En la actualidad, el banco ha eliminado la complejidad de los usuarios de VPN y dispositivos móviles gracias a la integración de una moderna plataforma de administración de dispositivos móviles y la optimización de credenciales en una sola aplicación de tarjetas inteligentes para dispositivos móviles supervisada por un servicio de PKI. "El equipo de TI está reduciendo lentamente la cantidad de sistemas redundantes, comenzando por modernizar sus procesos de emisión de dispositivos y utilizando tarjetas inteligentes más alineadas con Active Directory", continuó el ingeniero de seguridad.

El paso a un servicio de PKI administrado también facilitó las cosas para el equipo de TI. "Con una infraestructura completamente in situ, el nivel de seguridad que intentamos alcanzar trajo aparejadas una serie de complejidades y gastos que no podíamos afrontar con nuestro personal", describió el ingeniero de seguridad. "A menos que se trate de una organización grande con equipos numerosos, la administración interna de un programa de PKI probablemente no sea una aventura muy conveniente".

Además, el equipo de TI interno está trabajando con el especialista en PKI para integrar la emisión de certificados con sus tarjetas inteligentes, y además ha reemplazado un sistema inconexo con un servicio administrado y optimizado para brindar soporte al correo electrónico seguro. La compañía administra su propia instancia de Active Directory, y sigue consolidando los procesos para administrar autoridades de certificados y publicar certificados. Como su plataforma de administración de tarjetas inteligentes ahora está integrada con la administración de certificados, se utilizan certificados digitales para brindar soporte al acceso a VPN. La adopción de una PKI administrada ha optimizado en gran medida la administración del ciclo de vida útil de los certificados en las 40 sucursales, liberando a los equipos de TI de otra tarea más para que puedan concentrarse en otros proyectos.

Un fabricante de alta tecnología opta por una PKI para brindar soporte de identidad de dispositivos y acceso a VPN con el fin de lograr un ambiente de confianza cero para activos críticos

Un proveedor de soluciones de administración de energía blindó su entorno gracias a las capacidades integradas del entorno de servicios de certificados de Microsoft Active Directory, ordenando que los dispositivos administrados se validen con certificados de dispositivo y su infraestructura de PKI. El objetivo era blindar el acceso a recursos críticos mediante un método para validar la autenticidad de los usuarios que solicitaran acceso a VPN en su entorno, y comprobando el estado de los dispositivos administrados antes de otorgar acceso a recursos de la red privada. La compañía quería garantizar una conectividad segura y acelerar el proceso para que los usuarios accedan a recursos de la compañía, independientemente de su ubicación. El uso de certificados digitales controla estrictamente a los empleados, ya que requiere un terminal completamente administrado para acceder a recursos críticos, y puede restringir a contratistas y partners comerciales emitiendo certificados de autenticación de usuarios configurados para restringir el acceso y, si es necesario, aplicar reglas de firewall.

"Nuestra posición de defensa se construye alrededor de claves increíblemente difíciles de extraer de los dispositivos Microsoft", explicó el CISO de la empresa, quien además agregó que el fabricante está realizando inversiones escalonadas hasta llegar al objetivo final de un entorno de "confianza cero". El desafío de administrar esto se compone de una implementación continua de equipos Mac en su red para ingenieros, marketing y otros casos de uso especiales. La compañía está trabajando con un especialista en PKI para diseñar una manera de implementar un certificado de autenticación para los equipos Mac, con el fin de garantizar que la clave privada se almacene de forma segura y no pueda exportarse.

A medida que avance la implementación en la compañía, se agregarán nuevos metadatos en certificados recién emitidos para permitir la identificación de dispositivos. Los certificados se aprovecharán como parte del proceso de autenticación y de la conectividad de VPN en la plataforma de administración de acceso web in situ. La compañía ve con buenos ojos la flexibilidad de la plataforma, mediante la cual los empleados pueden acceder a un portal que contiene Office 365 y otros recursos de la compañía desde sus dispositivos móviles.

El arquitecto de seguridad en jefe de la compañía es precavido al hablar sobre la autenticación de dispositivos móviles basada en certificados. "Que la compañía pueda colocar un certificado en un dispositivo no significa que todo lo que contiene ese dispositivo tenga la capacidad de interactuar con el certificado". Si el desarrollador de la aplicación no la ha programado de forma tal que pueda aprovechar un certificado implementado de forma general en un dispositivo, la aplicación jamás lo utilizará", explicó. Probablemente la aplicación no pueda recibir el certificado desde el dispositivo que posee el certificado. En vista de esto, la compañía está desarrollando una nueva estrategia de identidad de nube que brinde soporte a aplicaciones internas y a aplicaciones de terceros que consumen los empleados.

Los certificados digitales son fundamentales para la estrategia de movilidad de la compañía y para los requisitos de acceso remoto de los empleados

Una firma de prueba de productos electrónicos global utiliza una combinación de certificados para usuarios y dispositivos con el fin de otorgar acceso a recursos sensibles de la compañía en laptops y dispositivos móviles propiedad de la compañía y de los usuarios. El resultado es un sólido porcentaje de retención de empleados y un equipo de ingeniería innovador que, según el CISO, se enorgullece

de usar certificados digitales para mantener una posición de seguridad sólida que no obstaculiza la flexibilidad con la que deben contar los empleados para trabajar con comodidad.

"Decidimos que los certificados eran nuestro mejor componente, y que debíamos utilizarlos en distintos casos de uso. Como todos nuestros partners comerciales tienen certificados para la VPN, los usuarios también cuentan con ellos a través de la administración de dispositivos móviles para BYOD", agregó el CISO.

El trabajo más pesado vinculado con una PKI es lograr instalar cadenas de confianza que lleguen a todos los clientes. No hay interoperabilidad entre las implementaciones de PKI de la compañía, ya que ni los equipos de desarrollo e ingeniería de la compañía ni las operaciones de marketing y ventas de la compañía están interesados en explorar la interoperabilidad. Las operaciones de la compañía dependen de una cadena de confianza por separado para cada implementación de PKI. Por otra parte, un enfoque centralizado puede ser más eficiente y rentable, ya que solo debe implementarse una cadena de confianza.

Como parte de los esfuerzos de la compañía por mantener una seguridad sólida, la implementación de PKI para acceso móvil y a VPN está casi totalmente personalizado para perfiles de certificados del lado de Microsoft. Para reducir el riesgo de certificados robados y ataques de fuerza bruta diseñados para acceder a recursos críticos, la compañía desarrolló una vinculación de certificados personalizada. Cuando los usuarios inician sesión, solo ven un aviso para ingresar su contraseña, no un aviso de certificado. Esto hace que los certificados funcionen solo para usuarios individuales. Es una relación uno a uno para garantizar que un certificado y una contraseña jamás funcionen de forma conjunta. "En mi opinión, eso es un componente de seguridad esencial clave en una implementación de certificados", afirmó el CISO.

Un procesador de pagos protege miles de dispositivos POS con una PKI

Los fabricantes sufren una presión cada vez mayor por agregar mecanismos de seguridad basados en hardware y software a dispositivos de la Internet de las cosas con el fin de brindar soporte de cifrado, autenticación y autorización, y para validar la integridad del firmware del dispositivo, el sistema operativo y las aplicaciones. Los certificados digitales son los elementos de confianza utilizados para lograr este nivel fundacional de seguridad en sistemas integrados.

Un procesador de pagos en Europa está protegiendo decenas de miles de dispositivos de sistemas POS a través de un servicio de PKI administrado que permite la autenticación confiable, independiente y mutua de dispositivos en redes. El nuevo enfoque desarrollado por el procesador de pagos requiere la instalación de certificados digitales para identidad de dispositivos, y de un agente de dispositivos que pueda comunicarse con la plataforma basada en la nube del procesador de pagos. La plataforma se usa para aprovisionar, supervisar y mantener sistemas POS, y para establecer un mecanismo seguro de rotación de certificados.

Un arquitecto de seguridad que supervisa la implementación afirmó que el uso de certificados digitales reduce el fraude a nivel del fabricante y le brinda a su compañía más control sobre el uso de dispositivos. "Se optó por una PKI debido a que los certificados pueden administrarse en todo el ciclo de vida útil a volúmenes que pueden escalar", explicó. "Un requisito clave fue el establecimiento de una solución que no pudiera ser secuestrada por un atacante mediante el uso de certificados digitales fraudulentos", en palabras del arquitecto de seguridad. El mecanismo desarrollado garantiza que los datos inactivos o en tránsito estén protegidos, y valida que las entidades que envían y reciben información sean quienes dicen ser.

Además de mantener la supervisión del aprovisionamiento de archivos y la administración de credenciales en los sistemas de POS, la solución permite que el proveedor venda servicios orientados a políticas y garantiza que los vendedores no omitan sus obligaciones de cumplimiento.

Otros dispositivos de alto riesgo utilizados por el proveedor no admiten un enfoque basado en agentes. Un fabricante de sistemas integrados que trabaja junto con el procesador de pagos y otros envía productos que tienen el espacio ni la potencia para brindar soporte a un software de cliente o agente. El fabricante le dijo a IDC que su equipo de diseño utiliza PKI cuando se produce para brindar soporte a firma de código y comunicaciones de máquina a máquina. "Nuestros clientes nos solicitaron establecer una práctica para garantizar la integridad de cualquier código enviado a nuestros clientes", según el líder del equipo de seguridad, que trabajó junto con el equipo de ingeniería. El objetivo era seleccionar una solución de PKI en lugar de incorporarla en la implementación de PKI existente del fabricante.

"Hemos estado buscando formas de automatizar el proceso sin generar una carga adicional para el equipo que se encarga de nuestros procesos internos", agregó.

POR QUÉ ELEGIR DIGICERT

DigiCert es un proveedor de certificados digitales altamente confiables cuyo objetivo es simplificar las soluciones de SSL/TLS y PKI, identidad, autenticación y cifrado para la web y la Internet de las cosas (IoT). DigiCert brinda soporte para la creación automatizada de una configuración flexible de perfiles de certificados y métodos de inscripción y recuperación con custodia de clave segura que admite seguridad de correo electrónico. Los certificados se usan para validar la integridad del contenido de correo electrónico, garantizar la privacidad de los mensajes y probar la autoría de mensajes altamente críticos. Además, con frecuencia se usan certificados para brindar soporte de firma digital, con el fin de mantener la integridad de documentos legales, contratos y facturas críticos para el crecimiento y la continuidad de los negocios.

La plataforma DigiCert también permite que los administradores de TI tengan una estructura de administración centralizada para brindar soporte de acceso seguro al trabajo desde cualquier lugar y en cualquier momento. La plataforma se utiliza ampliamente para autenticar empleados en aplicaciones y sitios web, y permite que las organizaciones cuenten con la flexibilidad para diseñar perfiles de certificados y mecanismos de inscripción personalizados, con el fin de brindar soporte de VPN seguro, conectividad de red y movilidad con velocidad y escala. Además, se usa para proteger dispositivos móviles, correo electrónico móvil y aplicaciones con sus datos asociados. Esto permite que los administradores automaticen la inscripción y la emisión de certificados para, en última instancia, controlar el acceso a servicios empresariales, supervisar los controles de privacidad y administrar las restricciones de aplicaciones. La plataforma de PKI de DigiCert brinda soporte para IoT. De esa manera, las empresas pueden aprovisionar dispositivos conectados a escala y administrar certificados a través de un servicio de PKI en la nube, que ofrece almacenamiento seguro y administración de claves de certificados.

DESAFÍOS/OPORTUNIDADES

Las organizaciones han realizado inversiones de larga data en su infraestructura de PKI existente. Los profesionales de PKI entrevistados por PKI afirmaron que el proceso de optimización y automatización del frecuentemente complejo y fragmentado ecosistema de PKI que intentan mantener es una iniciativa

que debe encararse en varios frentes y durante varios años. Este esfuerzo requiere una inversión inicial, especialistas en PKI que conozcan los procesos comerciales y la infraestructura de TI existentes de la organización, la ubicación de los recursos críticos y la tolerancia a los riesgos existentes y la estrategia de crecimiento de la gerencia. El crecimiento rápido, las fusiones y las adquisiciones, la adopción de nuevas tecnologías, los cambios de estrategia comercial y otros factores externos pueden tener un impacto profundo e incluso hacer fracasar estos proyectos de mejora si no se planifican de forma adecuada y se ejecutan sistemáticamente.

CONCLUSIÓN

Dado el aumento continuo en la adopción de la nube y la cantidad de organizaciones que administran el acceso a datos y otros recursos corporativos en entornos híbridos y multinube, se recurrirá cada vez más a la tecnología de PKI, que desempeñará un rol clave para validar la integridad de las transacciones comerciales y establecer una conexión segura y confiable entre seres humanos y sistemas. Los datos de la *Encuesta de servicios de datos para la nube híbrida* de IDC valida esto. En 2010, el 32 % de las organizaciones con más de 10 000 empleados indicaron que habían usado PKI como parte de sus programas de seguridad. En 2018, el 65 % de las grandes empresas afirmaron haber ejecutado una implementación total y robusta en todos los almacenes de datos y recursos correspondientes. Las conclusiones clave que sugieren los motivos de la mayor importancia de la PKI son las siguientes:

- **Escalabilidad:** las personas entrevistadas en este estudio aprovecharon el tamaño y la escala considerables de PKI y nos brindaron datos sobre el tamaño de su base de usuarios, la cantidad de dominios y los volúmenes de las solicitudes de autenticación. Estas organizaciones de TI debieron enfrentar requisitos de escala considerables. Todos los entrevistados del sector corporativo, con un rango entre 1000 y 120 000 empleados, expresaron satisfacción con el rendimiento y la viabilidad, y tenían confianza en un crecimiento continuo posibilitado por la tecnología de PKI en cuanto a sus necesidades futuras de movilidad, acceso remoto, conectividad inalámbrica segura, firma de documentos, cifrado y correo electrónico seguro.
- **Servicios de PKI administrados:** los problemas y las inquietudes existentes estaban asociados con las distintas implementaciones de la tecnología PKI, algo que creaba complejidades y también una falta de ingenieros de redes y seguridad capacitados para manejarlas. Este contexto está impulsando la adopción de servicios de PKI administrados, con el fin de aumentar el personal existente y limitar la disrupción que provocan las actividades de PKI comunes, como la incorporación de nuevos empleados y la emisión y la revocación de certificados.
- **Sofisticación de atacantes:** los entrevistados afirmaron que, cuando una PKI se integra y "no se rompe", frecuentemente sus equipos de TI prefieren no tocarla. Pero está claro que la mayor complejidad y la falta de una supervisión proactiva provoca vulnerabilidades y problemas de configuración que pueden aprovechar los atacantes. Al aprovechar las debilidades de configuración, los atacantes pueden realizar un ataque tipo "man-in-the-middle" para vigilar a determinados empleados o, en un escenario más probable, robar datos sensibles para obtener beneficios económicos.

En este estudio de IDC, se descubrió que la PKI es esencial para proteger iniciativas de transformación digital en distintas empresas y casos de uso. Los procesos comerciales de hoy pueden contar con el soporte de una PKI para aumentar la automatización, reducir la fricción y optimizar el procesamiento de información digital y transacciones electrónicas. La PKI también es un elemento

esencial que utilizan los equipos de seguridad que deben enfrentar nuevas regulaciones de privacidad y seguridad de datos. Los CISO están de acuerdo en que las implementaciones de PKI optimizadas reducen la complejidad, y en que la adopción de servicios de PKI optimizados puede reducir los gastos y los costos de administración, liberando a los equipos de seguridad para que trabajen en otros asuntos más urgentes. Además, este estudio sirvió para validar que los certificados digitales son componentes esenciales que pueden frustrar ataques dirigidos y ayudar a garantizar la integridad de transacciones sensibles, y también a asegurarse de que las partes involucradas en transacciones comerciales sean quienes dicen ser. Lo que es más importante, el estudio llegó a la conclusión de que la PKI se usa como facilitador de nuevos proyectos de negocios diseñados para mejorar la satisfacción del cliente, con el fin de que puedan realizar transacciones más sensibles desde la comodidad de sus hogares.

Acerca de IDC

International Data Corporation (IDC) es el principal proveedor del mundo de inteligencia de mercado, servicios de consultoría y eventos para los mercados de tecnología de la información, telecomunicaciones y tecnología del consumidor. IDC ayuda a que profesionales de TI, ejecutivos de negocios y la comunidad de inversores tome decisiones informadas y basadas en hechos vinculadas con las compras de tecnología y la estrategia comercial. Más de 1100 analistas de IDC aportan su experiencia global, regional y local sobre tecnología, oportunidades y tendencias en el sector en más de 110 países. Durante 50 años, en IDC hemos proporcionado panoramas estratégicos a nuestros clientes para ayudarles a lograr sus objetivos comerciales clave. IDC es una subsidiaria de IDG, la compañía líder mundial en eventos, investigación y medios de tecnología.

Sede central global

5 Speen Street
Framingham, MA 01701
EE. UU.
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com