WHITE PAPER

Garantía de seguridad de la identidad digital:

cómo proteger los datos de sus clientes

Resumen ejecutivo

La gestión de la identidad digital y los perfiles de cliente constituyen el germen de la transformación digital de cualquier empresa. Las identidades de cliente, y los datos personales asociados a ellas, forman parte de los recursos más valiosos que cualquier empresa necesita. Proteger estas identidades digitales, desde el registro hasta las etapas posteriores de la relación con el cliente, y garantizar el valor empresarial continuo de los datos asociados es fundamental para tener éxito.

A la hora de gestionar identidades digitales y entablar una relación de confianza con el consumidor, las empresas deben aplicar las medidas de seguridad más estrictas para protegerse a sí mismas y a sus clientes. En el peor de los casos, los clientes podrían convertirse en víctimas de robo de identidad, con consecuencias potencialmente trágicas para su seguridad financiera, profesional y personal. Entonces, el cliente no solo podría dejar de confiar en la empresa, sino que podría exigirle responsabilidad e interponer una demanda judicial colectiva.

Además, las empresas deben aplicar estrictas medidas de protección de los datos personales para cumplir con las normativas internacionales de privacidad, como el Reglamento General de Protección de Datos (RGPD)[1] de la Unión Europea, la Ley de Privacidad del Consumidor de California (CCPA, California Consumer Privacy Act)[2], la Ley de Protección de Datos Personales y Documentos Electrónicos canadiense (PIPEDA, Personal Information Protection and Electronic Documents Act)[3] y otras normativas específicas del sector, como las leyes de privacidad que tratan la seguridad de la información médica.

En este documento se analizan:

- *La necesidad de proteger las identidades de los consumidores con una solución de gestión de acceso e identidades de cliente (CIAM) y una infraestructura sólida y segura.*
- *La necesidad de una funcionalidad de seguridad avanzada y flexible, como el acceso delimitado.*
- *La importancia de la protección de la red en el borde de Internet.*
- *El cada vez mayor número de normativas internacionales en materia de privacidad.*
- *Cómo generar confianza en el consumidor.*
- *Las ventajas de una solución CIAM basada en la nube.*

El documento concluye con un breve ejemplo real de una empresa farmacéutica líder a nivel mundial que implementó una solución CIAM segura y de primera clase para dotar a sus proveedores de servicios sanitarios de las mejores normativas en materia de privacidad de datos.

Identidades de cliente seguras

Las identidades digitales de los clientes son activos valiosos. Las empresas utilizan cada vez más los datos de identidad para personalizar la experiencia de los clientes en función de las preferencias, el comportamiento y los aspectos demográficos. Si bien la recopilación de datos de identidad destinada a personalizar las experiencias ha beneficiado tanto a las empresas como a los clientes, también ha aumentado el riesgo de que se produzcan filtraciones de datos costosas y perjudiciales para la marca.

En el informe sobre el coste de las filtraciones de datos de 2019, realizado por IBM Security y Ponemon Institute, se descubrió que el 48 % de las organizaciones representadas identificaban un ataque malicioso o delictivo como la causa principal de una filtración de datos, con un coste medio de aproximadamente 157 dólares por cada registro de identidad filtrado[4]. Como las vulneraciones de la seguridad de la información personal afectan con frecuencia a cientos de miles, o incluso millones, de registros de clientes, el coste resultante puede dañar gravemente a una empresa, sin contar la posible pérdida de ingresos por daños a la reputación de la marca y la pérdida de confianza de los clientes.

La recopilación y el almacenamiento de datos de clientes (es decir, el mantenimiento y procesamiento de credenciales de clientes e información personal) implica un deber de diligencia que las empresas y las organizaciones no pueden permitirse vulnerar ni poner en peligro. Como responsabilidad añadida, los Gobiernos han introducido una legislación para proteger la información de identificación personal (PII) de los clientes. El RGPD de la Unión Europea, la CCPA de California y la PIPEDA de Canadá son solo algunas de las muchas normativas de privacidad de datos que se aplican internacionalmente.

Para que una marca global se adhiera a los matices de las diferentes normativas regionales sobre privacidad de datos, debe perfilar una estrategia con la que se recopile, procese y almacene PII de forma detallada de acuerdo con la ley correspondiente, o bien optar por revisar su estrategia de privacidad de datos para el cumplimiento global.

Además de proteger la identidad de cada uno de los clientes, la propia infraestructura de TI subyacente debe estar protegida de amenazas, como los ataques distribuidos de denegación de servicio (DDoS) que, de otro modo, podrían provocar tiempos de inactividad, la degradación del rendimiento, la pérdida de confianza de los clientes y posibles pérdidas financieras. La recopilación de determinados datos de clientes puede ayudar, de hecho, a proteger la infraestructura. Por ejemplo, la dirección IP utilizada por un cliente se puede registrar y comprobar en una lista negra para evitar actividades fraudulentas. Muchas de las normativas de privacidad más recientes, como el RGPD, consideran que las direcciones IP son información personal, pero permiten recopilar y procesar dichos datos siempre que solo se haga con fines de seguridad.

Protección de los datos de los clientes

Para proteger los datos de los clientes y mantener su confianza, las empresas deben empezar con una solución CIAM de primera clase que garantice un cifrado sólido de los datos y credenciales de los usuarios, y un control de acceso delimitado. Tanto si se crea una solución CIAM interna como si se implementa una solución comercial de uso profesional, las organizaciones deben asegurarse de que su solución de gestión de identidades sea capaz de hacer lo siguiente:

- *Proteger los datos, en tránsito o en reposo, de los clientes con un cifrado seguro.*

- *Proporcionar un control de acceso delimitado tanto para datos como para aplicaciones. Debe ser posible controlar el acceso incluso a campos de registro de datos concretos (en lugar de sistemas que solo permiten "o todo o nada") y por rol o atributo.*
- *Proteger las cuentas de los clientes contra el abuso mediante métodos de autenticación de usuarios sólidos, como la autenticación incremental y por contraseñas de un solo uso (OTP), y mediante pruebas de desafío-respuesta de tipo CAPTCHA.*
- *Detener el tráfico de ataques antes de que pueda llegar a aplicaciones esenciales y provocar cortes de servicio, degradar el rendimiento o aumentar los costes informáticos.*
- *Cumplir las certificaciones y las normativas de protección de seguridad, como las normas de la Organización Internacional de Normalización (ISO) 27001:2013 y 27018:2014, los Controles de Organizaciones de Servicio (SOC) 2 de tipo II y la Cloud Security Alliance (CSA) STAR de nivel 2.*
- *Permitir el cumplimiento total de las diferentes normativas regionales de privacidad de datos, lo que incluye el RGPD, la CCPA, la PIPEDA y muchas otras normativas específicas del sector y de asistencia sanitaria.*

Control de acceso delimitado

Para proteger la información de identidad del cliente, las soluciones CIAM deben proporcionar niveles de permiso muy detallados para garantizar un control total de las personas y las aplicaciones que pueden acceder a la información y tratarla, todo ello basado en roles y responsabilidades.

El control de acceso detallado debe aplicarse a todas las columnas, filas y campos de datos. Por ejemplo, debería ser posible definir roles que permitan a los desarrolladores realizar tareas de administración de aplicaciones sin permitirles acceder a ningún dato de cliente.

Además, una solución CIAM debe ofrecer un conjunto de roles predefinidos basados en las obligaciones administrativas habituales que sustenten el principio de privilegio mínimo: por ejemplo, roles específicos para los representantes del servicio de atención al cliente que necesitan acceder a datos de clientes sin más permisos administrativos.

Dicho acceso delimitado debe estar disponible para los empleados y contratistas de la empresa, así como para las aplicaciones de ventas y marketing de la organización. Esto puede ser muy útil para evitar la diseminación de datos tóxicos. Por ejemplo, si un usuario opta por no recibir comunicaciones por correo electrónico, una solución CIAM con acceso delimitado puede bloquear automáticamente el acceso a los sistemas de automatización del marketing y a otras instalaciones para que no accedan a la dirección de correo electrónico de dicho usuario.

Protección en el borde de Internet

Un componente importante de la seguridad de la identidad digital es la protección de la red en el borde de Internet. Las soluciones CIAM empresariales deben proteger los terminales de registro frente a amenazas cada vez más complejas y sofisticadas, que van desde intentos avanzados y oportunistas de filtrar datos hasta ataques DDoS y llamadas maliciosas a interfaces de programación de aplicaciones (API).

Al tener capas de protección en los terminales de identidad y protegerlos en el borde de Internet, se pueden detectar y descartar actividades y agentes maliciosos antes de que estos (y el tráfico de ataques potencialmente masivo que provocan) puedan llegar a los sitios web y aplicaciones reales.

Para aumentar el rendimiento en todo lo relacionado con la gestión de identidad, las soluciones empresariales deben aplicar tecnología de almacenamiento en caché inteligente a fin de mantener los datos cerca de los usuarios finales y garantizarles una experiencia positiva.

Las normativas de privacidad y la confianza

Estrechamente relacionado con el concepto de seguridad de identidad digital encontramos el concepto de garantía de privacidad del cliente. Tal y como se explica en el white paper complementario "Más allá del RGPD y la CCPA: El control de las identidades ayuda a las empresas a cumplir la ley y aumentar la confianza de sus clientes", se está promulgando a un ritmo apresurado un número creciente de normativas de privacidad, como el RGPD y la CCPA, que está motivado por toda una serie de filtraciones de datos, robos de identidad y otros escándalos relacionados que han recibido una gran atención mediática[5]. Solo en EE. UU., 10 estados han introducido o aprobado proyectos de ley que imponen obligaciones empresariales de gran alcance para proporcionar a los clientes mayor transparencia y mejor control sobre su información personal[6].

Las empresas no pueden permitirse ignorar estas nuevas leyes y normativas sobre privacidad. Solo desde el punto de vista financiero, las multas moderadas que se impusieron durante los primeros 12 meses de vigencia del RGPD han dado paso a multas mucho mayores. La multa reciente de 123 millones de dólares impuesta a una empresa hotelera internacional debido al pirateo de información personal de 380 millones de huéspedes es un ejemplo excelente[7]. Y estas multas están destinadas a aumentar su tamaño, hasta el exorbitante límite estatutario que establece el RGPD de un 4 % de la facturación mundial anual.

Sin embargo, el coste para las empresas globales es mucho más que económico. Está en riesgo la confianza del cliente. Hoy en día, las empresas necesitan un consentimiento explícito para procesar los datos personales. Y el consentimiento requiere confianza. Sin confianza, no hay consentimiento. Sin consentimiento, no hay datos. Y eso lleva a campañas de ventas y marketing ineficaces.

Respetar la seguridad y la privacidad no es solo una cuestión de cumplimiento, sino también una ventaja empresarial clave. La seguridad, el control de la privacidad y la gestión de identidades ayudan a las empresas a establecer una relación estrecha con usuarios y clientes, lo que se traduce en una mayor fidelidad y en la posibilidad de que la empresa obtenga unos ingresos más elevados.

La necesidad de contar con una CIAM innovadora

De acuerdo con el RGPD y otras legislaciones en materia de privacidad, las organizaciones que procesan datos personales deben proteger estos contra el acceso no autorizado. Ser capaz de demostrar que se están protegiendo eficazmente los datos mediante medidas de seguridad "adecuadas" e "innovadoras" es esencial para cumplir con el RGPD.

Pero ¿qué es una "medida de seguridad adecuada" y qué pruebas se esperan? Según el RGPD, se consideran medidas de seguridad adecuadas las que tienen en cuenta la "innovación", el coste de implantación, el alcance, el contexto y los fines del procesamiento de los datos, y que valoren todos

estos factores con respecto a los riesgos y el impacto en las libertades de los individuos. Por lo tanto, una organización debe determinar qué es apropiado o proporcionado y, claro está, tendrá que hacer referencia a las prácticas recomendadas del sector como guía.

Una herramienta que permite determinar el equilibrio adecuado es la evaluación del impacto de la protección de datos (EIPD)[8], proceso aplicable en determinados casos según el RGPD que determina el impacto potencial de las operaciones de procesamiento de datos. Para realizar una EIPD, una organización deberá documentar en detalle una serie de factores, entre otros:

- *Las operaciones de procesamiento de datos previstas.*
- *La necesidad y el alcance de estas operaciones.*
- *Una evaluación de los riesgos de filtración de datos asociados a las operaciones.*
- *Las medidas previstas para hacer frente a estos riesgos, incluidos los mecanismos y las medidas de seguridad adoptados para garantizar la protección de los datos personales.*

El RGPD y otras normativas exigen un enfoque basado en el riesgo para la protección de datos. No hay una fórmula fija que se pueda aplicar a todos los casos: las obligaciones en lo que respecta a la seguridad de los datos deben desarrollarse tras exhaustivos análisis de los riesgos inherentes a cada operación de procesamiento para cada uno de los interesados.

Si bien este enfoque ofrece la flexibilidad necesaria para que las organizaciones puedan aplicar medidas razonables en función de los costes, la arquitectura del sistema y otros factores, también exige una revisión en profundidad de coste-beneficio/riesgos de todas las actividades relacionadas con los datos personales.

El grado de éxito con el que una organización pueda o no proporcionar prueba suficiente de la mitigación eficaz de los riesgos dependerá del nivel de conocimiento que tenga de los riesgos significativos para la privacidad, además de la eficiencia de las medidas de seguridad y gestión de datos "innovadoras" que decida aplicar en respuesta a los riesgos percibidos.

Las ventajas de la nube

Para implementar los conceptos, procesos y tecnologías de seguridad de la identidad digital que se tratan en este documento, las empresas tienen dos opciones básicas: desarrollar internamente una solución empresarial o adquirirla de un proveedor especializado en CIAM.

Tal y como se analiza ampliamente en el white paper "Desarrollar o comprar: Guía de la gestión de acceso e identidades de cliente", las soluciones comerciales y basadas en la nube suelen ser la mejor opción para los objetivos, necesidades y recursos de la mayoría de las empresas[9]. En especial, este es el caso de la implementación inicial, así como el nivel de esfuerzo necesario para utilizar y mantener una solución a largo plazo con requisitos en constante cambio dictados por la tecnología, los consumidores, los mercados y los organismos reguladores. En concreto, las cláusulas más innovadoras de la legislación reguladora, como el RGPD, se cumplen mejor con las soluciones de terceros de calidad profesional.

Las soluciones CIAM comerciales tienen varias ventajas significativas con respecto a los departamentos de TI internos, desde una labor de I+D continua hasta SLA garantizados. Las soluciones en la nube añaden una escalabilidad elástica, procesos de failover multirregionales y recuperación ante desastres, así como niveles de seguridad muy superiores a los que pueden lograr los equipos internos.

Las soluciones CIAM comerciales presentan ciertas ventajas relevantes frente a los departamentos de TI internos que tratan de desarrollar una solución propia. No se trata solo de que ofrezcan disponibilidad global y escalabilidad o que cumplan los acuerdos de nivel de servicio (SLA) y las certificaciones de seguridad: las soluciones CIAM comerciales cuentan con la experiencia, los recursos y la investigación y desarrollo constantes que ofrecen los proveedores externos, lo que permite que los equipos de TI internos se concentren en impulsar otras iniciativas clave para la empresa.

Las soluciones CIAM diseñadas con el objetivo de aprovechar el potencial de una nube moderna para compartir recursos, proporcionar escalabilidad elástica, garantizar la seguridad y posibilitar procesos de failover multirregionales y recuperación ante desastres también ofrecen funciones de identidad como servicio (IDaaS) con infinidad de prestaciones, así como niveles de seguridad muy superiores a los que se pueden lograr con soluciones desarrolladas de forma interna. Como colofón, no es necesario que la empresa posea ni opere hardware ni instalaciones de centros de datos.

Por mucho que las soluciones de gestión de identidades "caseras" parezcan un proyecto factible, se corre el riesgo de infravalorar la cantidad de esfuerzo, financiación, recursos internos y conocimientos que es indispensable invertir a largo plazo para asegurar su solidez, al tiempo que se mantiene y se mejora la solución para adaptarse a los inestables requisitos del mercado y a las expectativas de los consumidores.

Los proveedores de CIAM comerciales están mejor posicionados para adoptar los cambios que imponen los avances tecnológicos, los consumidores, los mercados o los organismos reguladores. No es ningún misterio: si un proveedor de soluciones quiere ofrecer un catálogo competitivo que cumpla con la normativa y no perder relevancia, debe desarrollar sus servicios constantemente. A medida que desarrollan sus soluciones no solo para uno, sino para muchos clientes, pueden obtener ventajas de la economía de escala que simplemente no están disponibles al desarrollar soluciones internas.

Una farmacéutica multinacional implementa una solución de gestión segura de identidades para capacitar a los proveedores de atención sanitaria

El desafío

Una farmacéutica multinacional de primer nivel colabora con proveedores de atención sanitaria, Gobiernos y comunidades locales para fomentar e impulsar un acceso fiable y asequible a los servicios sanitarios en todo el mundo. Sin embargo, múltiples normativas de cumplimiento en materia de promoción de productos y servicios para dichos proveedores comenzaron a afectar a sus objetivos de comercialización rápida de los tratamientos. La empresa necesitaba una solución de gestión de identidades que permitiera a los proveedores sanitarios acceder de manera segura y sin problemas a su sitio web profesional para aprovechar las promociones de fármacos con receta, respetando en todo momento las normativas locales. Para satisfacer estas necesidades, la empresa necesitaba una solución CIAM innovadora pensada específicamente para el ámbito corporativo.

La solución

La empresa se decantó por Akamai Identity Cloud para ofrecer un registro de cuentas seguro y totalmente personalizado en su sitio web profesional con flujos de trabajo de acceso, inicio de sesión único, autenticación, gestión de contraseñas, flujos de creación de cuentas, validación de campos, etc. Las funciones de gestión de perfiles permiten editar fácilmente la información de los perfiles, y la funcionalidad de almacenamiento de datos del perfil recopila y almacena automáticamente los datos de los proveedores en una base de datos en la nube segura, flexible y unificada.

La plataforma Identity Cloud es nueve veces más rápida que la solución anterior de la empresa. Gracias a esta solución, se ha podido ofrecer a todos los proveedores, independientemente de su ubicación geográfica, un acceso seguro e idéntico a los recursos médicos regulados, sin descuidar en ningún momento el cumplimiento de las distintas normativas locales sobre seguridad y conformidad. Ahora los proveedores pueden obtener muestras de fármacos en cuestión de días, en lugar de semanas, a través del sitio web seguro, con lo que se mejoran la atención a los pacientes y su calidad de vida. Por su parte, los representantes de la empresa ahora perciben mejoras en la productividad, al tener que realizar menos visitas a las oficinas de los proveedores para entregarles las muestras de los fármacos y otros recursos.

Además, las integraciones de Identity Cloud con las plataformas de tecnología de marketing existentes han permitido que la farmacéutica personalice sus iniciativas de marketing y las adapte a los proveedores a nivel mundial.

Akamai Identity Cloud

Identity Cloud es la solución de Akamai para CIAM. La plataforma proporciona todo lo que las empresas necesitan para que sus clientes puedan crear cuentas personales e iniciar sesión de forma segura en sitios web, aplicaciones móviles o aplicaciones basadas en el IoT. Identity Cloud proporciona herramientas que se pueden utilizar para reducir de forma significativa los esfuerzos necesarios para el cumplimiento de normativas de privacidad, al tiempo que proporciona a las empresas un repositorio de perfiles de clientes muy seguro y permite una visión integral del cliente.

Identity Cloud ofrece capacidades y experiencias de usuario específicas que pueden ayudar a las empresas a cumplir los requisitos normativos y de seguridad. Las funciones de protección y privacidad de Identity Cloud incluyen registro de clientes, acceso, autenticación, inicio de sesión único, control de acceso delimitado, gestión de preferencias y consentimiento y muchas otras funciones necesarias para recopilar, gestionar y proteger datos personales.

Al implementar Identity Cloud, las empresas y las organizaciones pueden implementar la gestión de identidades empresarial de forma rápida y flexible. Diseñada con una arquitectura nativa de la nube, la solución se amplía de forma inteligente en función de las exigencias para adaptarse a los picos de tráfico y ofrecer escalabilidad a cientos de millones de usuarios, así como seguridad, rendimiento y disponibilidad para satisfacer las necesidades de las aplicaciones esenciales para la empresa. Akamai Identity Cloud se ha diseñado para ayudar a las organizaciones a cumplir las normativas internacionales de seguridad y privacidad, fomentar la confianza en su marca, gestionar los datos de los clientes y mitigar los riesgos, al lograr que los datos estén disponibles de forma segura en todas las regiones y aplicaciones.

Conclusión

Aparte del cumplimiento de las normativas al respecto, la privacidad y la seguridad de las identidades de los clientes son cruciales para las organizaciones que desean establecer una relación digital sólida y fiable con sus clientes en el entorno digital. Los consumidores tienen expectativas cada vez más altas y esperan que sus datos personales mantengan su confidencialidad y estén protegidos. Los numerosos casos conocidos de abuso de datos, vulneraciones y robos de identidad han elevado enormemente el listón para que las empresas puedan demostrar que son depositarios de confianza de los datos personales. Cuando los clientes entregan sus datos a una organización, suscriben un contrato de confianza. Si se infringe esa confianza, es muy difícil restablecerla.

FUENTES

1) Normas de protección de datos de la Unión Europea, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_es
2) Información legislativa de California: Ley de Privacidad AB-375, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
3) Ley de Protección de Datos Personales y Documentos Electrónicos (PIPEDA), https://www.privac.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
4) IBM 2019 Cost of a Data Breach Report, https://www.ibm.com/security/data-breach
5) White paper de Akamai: Más allá del RGPD y la CCPA: El control de las identidades ayuda a las empresas a cumplir la ley y aumentar la confianza de sus clientes https://www.akamai.com/es/es/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf
6) Davis Wright Tremaine: "Copycat CCPA" Bills Introduced in States Across Country, https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet: Marriott Faces $123 Million GDPR Fine in the UK for Last Year's Data Breach, https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
8) Data Protection Impact Assessment (DPIA): How to Conduct a Data Protection Impact Assessment, https://gdpr.eu/data-protection-impact-assessment-template/
9) White paper de Akamai: Desarrollar o comprar: Guía de la gestión de acceso e identidades de cliente, https://www.akamai.com/es/es/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf

Akamai garantiza experiencias digitales seguras a las empresas más importantes del mundo. La plataforma inteligente de Akamai en el Edge llega a todas partes, desde la empresa a la nube, para garantizar a nuestros clientes y a sus negocios la máxima eficacia, rapidez y seguridad. Las mejores marcas del mundo confían en Akamai para lograr su ventaja competitiva gracias a soluciones ágiles que permiten destapar todo el potencial de sus arquitecturas multinube. En Akamai mantenemos las decisiones, las aplicaciones y las experiencias más cerca de los usuarios que nadie; y los ataques y las amenazas, a raya. La cartera de soluciones de seguridad perimetral, rendimiento web y móvil, acceso empresarial y distribución de vídeo de Akamai está respaldada por un servicio de atención al cliente y análisis excepcional, y por una supervisión ininterrumpida, durante todo el año. Para descubrir por qué las marcas más importantes del mundo confían en Akamai, visite www.akamai.com o blogs.akamai.com, o siga a @Akamai en Twitter. Puede encontrar los datos de contacto de todas nuestras oficinas en www.akamai.com/locations. Publicado en noviembre de 2019.