WHITEPAPER

Sicherheit für digitale Identitäten:

So schützen Sie die Daten Ihrer Kunden

Zusammenfassung

Die Verwaltung von digitalen Identitäten und Kundenprofilen steht im Mittelpunkt der digitalen Transformation eines jeden Unternehmens. Die Identität der Kunden und die damit verbundenen persönlichen Daten zählen zu den wichtigsten und wertvollsten Ressourcen jedes Unternehmens. Die Sicherung dieser digitalen Identitäten – von der Registrierung bis zu späteren Phasen der Kundenbeziehung – und die Gewährleistung des kontinuierlichen geschäftlichen Nutzens aus den zugehörigen Daten sind für den Geschäftserfolg von entscheidender Bedeutung.

Bei der Verwaltung digitaler Identitäten und beim Aufbau von Kundenvertrauen müssen Unternehmen strengste Sicherheitsmaßnahmen ergreifen, um sich und ihre Kunden zu schützen. Im schlimmsten Fall können Kunden Opfer eines Identitätsdiebstahls werden, was sich unter Umständen erheblich auf ihre finanzielle, berufliche und persönliche Sicherheit auswirkt. All dies kann nicht nur zu einem Vertrauensverlust führen, sondern auch zu Haftungsansprüchen und Klagen gegen das Unternehmen.

Darüber hinaus müssen Unternehmen strenge Identitätsschutzmaßnahmen zur Einhaltung internationaler Datenschutzvorschriften implementieren. Dazu gehören die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union[1], der California Consumer Privacy Act (CCPA)[2], der kanadische Personal Information Protection and Electronic Documents Act (PIPEDA)[3] und andere branchenspezifische Bestimmungen wie Datenschutzgesetze zur Sicherheit medizinischer Informationen.

In diesem Whitepaper werden folgende Themen behandelt:

- *Die Notwendigkeit, Verbraucheridentitäten mit Kundenidentitäts- und Zugriffsverwaltung (Customer Identity and Access Management, CIAM) und einer sicheren, robusten Infrastruktur zu schützen*
- *Der Bedarf an erweiterten, flexiblen Sicherheitsfunktionen wie die Beschränkung des Zugriffs*
- *Die Bedeutung von Edge-Netzwerkschutz*
- *Die Zunahme internationaler Datenschutzbestimmungen*
- *Der richtige Aufbau von Kundenvertrauen*
- *Die Vorteile cloudbasierter CIAM-Lösungen*

Der Artikel endet mit einem kurzen Praxisbeispiel eines weltweit führenden Pharmaunternehmens, das eine erstklassige, sichere CIAM-Lösung implementiert hat, um Gesundheitsdienstleister bei der Einhaltung von Datenschutzbestimmungen zu unterstützen.

Sichere Kundenidentitäten

Digitale Kundenidentitäten sind wertvolle Ressourcen. Unternehmen nutzen immer häufiger Identitätsdaten, um das Kundenerlebnis auf Grundlage von Vorlieben, Verhalten und demografischen Daten zu personalisieren. Die Erfassung von Identitätsdaten zur Personalisierung der Nutzererlebnisse kommt sowohl Unternehmen als auch Verbrauchern zugute, steigert jedoch auch das Risiko kostspieliger, markenschädigender Datenschutzverletzungen.

Laut der Studie „Cost of a Data Breach" („Kosten durch Datendiebstahl") aus dem Jahr 2019, die von IBM Security und dem Ponemon Institute erstellt wurde, war bei fast der Hälfte der befragten Unternehmen (48 Prozent) ein böswilliger oder krimineller Angriff Grundursache eines Datendiebstahls. Dabei beliefen sich die durchschnittlichen Kosten auf 157 US-Dollar pro gestohlener Datensatz.[4] Da Verstöße häufig Hunderttausende (oder sogar Millionen) von Datensätzen umfassen, können die daraus resultierenden Kosten den betreffenden Unternehmen erheblichen Schaden zufügen – selbst wenn die Umsatzeinbußen durch Image-Schäden und Vertrauensverlust außer Acht gelassen werden.

Die Erfassung und Speicherung von Kundendaten – und die Verarbeitung von Kundenanmeldeinformationen und personenbezogenen Daten – unterliegen einer Sorgfaltspflicht, die Unternehmen unter keinen Umständen vernachlässigen dürfen. Zusätzlich haben Regierungen Gesetze zum Schutz der personenbezogenen Daten von Kunden eingeführt. Die DSGVO der Europäischen Union, der kalifornische CCPA und der PIPEDA in Kanada sind nur einige der vielen Datenschutzbestimmungen, die weltweit eingeführt wurden.

Damit eine globale Marke die Nuancen der verschiedenen regionalen Datenschutzbestimmungen einhalten kann, muss sie eine Strategie implementieren, nach der personenbezogene Daten detailliert gemäß den entsprechenden Gesetzen erfasst, verarbeitet und gespeichert werden, oder ihre Datenschutzstrategie für globale Compliance überarbeiten.

Neben dem Schutz einzelner Kundenidentitäten muss die zugrunde liegende IT-Infrastruktur vor Bedrohungen wie DDoS-Angriffen (Distributed Denial-of-Service) geschützt werden, die andernfalls zu Ausfällen, reduzierter Performance, Vertrauensverlust der Verbraucher und potenziellen finanziellen Schäden führen können. Die Erhebung bestimmter Kundendaten kann sogar zur Sicherung der Infrastruktur beitragen. Beispielsweise kann die von einem Kunden verwendete IP-Adresse aufgezeichnet und gegen eine Blacklist überprüft werden, um betrügerische Aktivitäten zu verhindern. Viele der neueren Datenschutzbestimmungen wie die DSGVO betrachten IP-Adressen als personenbezogene Daten, erlauben jedoch die Erfassung und Verarbeitung solcher Daten, solange diese nur zu Sicherheitszwecken erfolgen.

Schutz von Kundendaten

Um Kundendaten zu schützen und das Vertrauen der Verbraucher zu wahren, sollten Unternehmen mit einer branchenführenden CIAM-Lösung beginnen, um Nutzer- und Anmeldedaten mit starker Verschlüsselung und bereichsbezogener Zugriffskontrolle zu sichern. Unabhängig davon, ob Unternehmen diese CIAM-Lösung intern erstellen oder eine professionelle kommerzielle Lösung implementieren, müssen sie sicherstellen, dass ihre Identitätsmanagement-Lösung folgende Vorteile bietet:

- *Schutz von Kundendaten mithilfer starker Datenverschlüsselung während der Übertragung und Speicherung*

- *Bereitstellung bereichsbezogener Zugriffskontrolle für Daten und Anwendungen. Die Zugriffskontrolle sollte bis auf die Ebene einzelner Datensatzfelder (im Gegensatz zu Systemen, die nur „nichts“ oder „alles“ zulassen) und nach Rolle und/oder Attribut möglich sein.*
- *Schutz von Kundenkonten vor Missbrauch dank starker Nutzerauthentifizierung wie Multi-Faktor- und OPT-Authentifizierung (One-Time Password) oder CAPTCHAs*
- *Abwehr von Angriffstraffic, bevor er kritische Anwendungen erreichen kann und Ausfälle verursacht, die Performance beeinträchtigt oder die Computing-Kosten in die Höhe treibt*
- *Einhaltung von Sicherheitszertifizierungen und -bescheinigungen wie International Organization for Standardization (ISO) 27001:2013 und 27018:2014, Service Organization Control (SOC) 2 Type II und Cloud Security Alliance (CSA) STAR Level 2*
- *Vollständige Compliance mit verschiedenen regionalen Datenschutzbestimmungen, einschließlich DSGVO, CCPA und PIPEDA sowie zahlreicher anderer branchenspezifischer und medizinischer Vorschriften*

Bereichsbezogene Zugriffskontrollen

Zum Schutz von Kundenidentitätsdaten sollten CIAM-Lösungen äußerst detaillierte Berechtigungsstufen bieten, um die vollständige Kontrolle darüber zu gewährleisten, welche Personen und Anwendungen auf Informationen zugreifen und diese bearbeiten können – und das alles basierend auf Rollen und Verantwortlichkeiten.

Eine detaillierte Zugriffskontrolle sollte bis hinunter zu Datenspalten, -zeilen und -feldern angewendet werden. Es sollte beispielsweise möglich sein, Rollen zu definieren, mit denen Entwickler Aufgaben zur Anwendungsverwaltung durchführen können, ohne ihnen Zugriff auf Kundendaten zu gewähren.

Darüber hinaus sollte eine CIAM-Lösung vordefinierte Rollen auf Grundlage typischer administrativer Aufgaben bieten, die das Prinzip geringstmöglicher Berechtigungen unterstützen, z. B. Rollen speziell für Kundendienstmitarbeiter, die ohne weitere Administratorberechtigungen auf Kundendaten zugreifen müssen.

Ein solcher beschränkter Zugriff sollte für Mitarbeiter und Auftragnehmer sowie für die Vertriebs- und Marketinganwendungen des Unternehmens verfügbar sein. Diese Funktion kann sehr hilfreich sein, um die Verbreitung gefährlicher Daten zu verhindern. Wenn ein Nutzer beispielsweise keine E-Mail-Kommunikation mehr erhalten möchte, kann eine CIAM-Lösung mit eingeschränktem Zugriff automatisch die E-Mail-Adressen dieser Person in den Marketing-Automatisierungssystemen und anderen Einrichtungen blockieren.

Schutz an der Edge

Eine wichtige Komponente der digitalen Identitätssicherheit ist der Schutz von Edge-Netzwerken. CIAM-Lösungen der Enterprise-Klasse müssen Registrierungsendpunkte vor immer komplexeren Bedrohungen schützen: von opportunistischen Angriffsversuchen bis hin zu DDoS-Angriffen und schädlichen API-Aufrufen (Application Programming Interface).

Wenn sich Schutzebenen in den Identitätsendpunkten des Netzwerks befinden und diese schützen, können schädliche Aktivitäten und böswillige Akteure erkannt und abgewehrt werden, bevor sie (und der potenziell massive Angriffstraffic, den sie verursachen können) die tatsächlichen Standorte und Anwendungen erreichen.

Um die Performance der Online-Erlebnisse in Verbindung mit digitalen Identitäten zu steigern, sollten Unternehmenslösungen auch intelligente Caching-Technologie anwenden, damit Daten und Erlebnisse nahe am Endnutzer gehalten werden.

Datenschutzbestimmungen und Vertrauen

Eng mit dem Konzept der digitalen Identitätssicherheit verknüpft ist das Konzept der Verbraucherschutzerklärung. Wie im begleitenden Whitepaper DSGVO, CCPA und andere Vorschriften zum Datenschutz: Wie Unternehmen mithilfe von Identity Governance das Vertrauen ihrer Kunden wahren und erhöhen beschrieben, werden weltweit immer mehr Datenschutzbestimmungen wie die DSGVO und der CCPA in rasantem Tempo umgesetzt. Dies wird durch medienwirksam publizierte Datenschutzskandale, Identitätsdiebstähle und ähnliche Vorfälle weiter vorangetrieben.[5] Allein in den USA haben zehn Bundesstaaten Gesetze eingeführt oder verabschiedet, die Unternehmen und Organisationen weitreichende Verpflichtungen auferlegen, um Verbrauchern mehr Transparenz und bessere Kontrolle über personenbezogene Daten zu bieten.[6]

Unternehmen können es sich nicht leisten, diese neuen Datenschutzgesetze und -vorschriften zu ignorieren. Allein aus finanzieller Sicht sind die moderaten Bußgelder, die in den ersten 12 Monaten der DSGVO erhoben wurden, mittlerweile deutlich höheren Bußgeldern gewichen. Die kürzlich gegen ein weltweit tätiges Gastgewerbeunternehmen verhängte Strafe in Höhe von 123 Millionen US-Dollar aufgrund eines Hackerangriffs auf die personenbezogenen Daten von 380 Millionen Hotelgästen stellt hierfür ein ausgezeichnetes Beispiel dar.[7] Und diese Geldstrafen können noch höher ausfallen – bis zur gestaffelten DSGVO-Obergrenze von 4 % des weltweiten Jahresumsatzes.

Die Kosten für globale Unternehmen sind jedoch weitaus höher als nur der finanzielle Aspekt. Gefährdet ist auch das Vertrauen der Verbraucher. Unternehmen benötigen heutzutage die ausdrückliche Einwilligung der Nutzer, um personenbezogene Daten verarbeiten zu können. Und diese Einwilligung erfordert Vertrauen. Ohne Vertrauen gibt es keine Einwilligung. Und ohne Einwilligung gibt es keine Daten. Und das führt zu ineffektiven Vertriebs- und Marketingkampagnen.

Die Sicherheit und die Einhaltung der Datenschutzbestimmungen sind nicht nur eine Frage der Compliance, sondern auch ein entscheidender Geschäftsvorteil. Sicherheit, Datenschutz und Identity Governance helfen Unternehmen dabei, enge Beziehungen zu Nutzern und Kunden aufzubauen, was zu einer höheren Kundenbindung und einem höheren Umsatzpotenzial führt.

Die Notwendigkeit moderner CIAM-Lösungen

Gemäß DSGVO und anderen Datenschutzgesetzen müssen Unternehmen, die personenbezogene Daten verarbeiten, diese Daten vor unbefugtem Zugriff schützen. Die Fähigkeit nachzuweisen, dass „angemessene" und „aktuelle" Sicherheitsmaßnahmen den Schutz der Daten effektiv gewährleisten, ist im Rahmen der DSGVO von entscheidender Bedeutung.

Aber was sind „angemessene" Sicherheitsmaßnahmen und welche Nachweise sind erforderlich?
Laut der DSGVO handelt es sich bei angemessenen Sicherheitsmaßnahmen um Maßnahmen, die den

Stand der Technik und die Implementierungskosten, den Umfang, den Kontext und den Zweck der Verarbeitung berücksichtigen und diese gegen die Risiken und die Auswirkungen auf die Rechte und Freiheiten von Einzelpersonen aufwiegen. Ein Unternehmen muss also entscheiden, was angemessen oder ausgewogen ist, und muss hierfür die Best Practices der Branche als Leitfaden heranziehen.

Ein Tool zur Bestimmung des richtigen Gleichgewichts ist die Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA)[8], ein Prozess, der in bestimmten Fällen im Rahmen der DSGVO erforderlich ist, um die potenziellen Auswirkungen von Datenverarbeitungsaktivitäten zu bestimmen. Bei einer DPIA muss ein Unternehmen eine Reihe von Faktoren im Detail dokumentieren, darunter die folgenden:

- *die geplanten Datenverarbeitungsvorgänge*
- *die Notwendigkeit und Verhältnismäßigkeit solcher Vorgänge*
- *eine Bewertung der Risiken eines Datendiebstahls bei solchen Vorgängen*
- *die vorgesehenen Maßnahmen, um diese Risiken zu minimieren, z. B. Schutzvorkehrungen und Sicherheitsmaßnahmen, um den Schutz personenbezogener Daten zu gewährleisten*

DSGVO und andere Vorschriften erfordern einen risikobasierten Ansatz für den Datenschutz. Datenbezogene Sicherheitsauflagen werden nicht in einem Vakuum vorgegeben, sondern müssen anhand einer gründlichen Analyse und in umfassender Kenntnis der Risiken entwickelt werden, die mit allen Datenverarbeitungsvorgängen für die betroffenen Personen verbunden sind.

Dieser Ansatz bietet die nötige Flexibilität, damit Unternehmen angemessene Maßnahmen ergreifen und dabei die Kosten, die Systemarchitektur und alle damit verbundenen Faktoren nicht aus dem Blick verlieren. Er erfordert jedoch eine rigorose Kosten-Nutzen-Risikoüberprüfung aller Vorgänge, die in Bezug auf personenbezogene Daten in Unternehmen stattfinden.

Wie erfolgreich ein Unternehmen ausreichende Nachweise für eine effektive Risikominimierung bereitstellen kann, hängt davon ab, wie gut es die relevanten Datenschutzrisiken abschätzen kann. Darüber hinaus müssen die modernen Datenverwaltungssysteme und Sicherheitsmaßnahmen, die das Unternehmen als Reaktion auf die wahrgenommenen Risiken einsetzt, höchst effektiv sein.

Die Vorteile der Cloud

Zur Implementierung der in diesem Dokument beschriebenen Konzepte, Prozesse und Technologien für die Sicherheit digitaler Identitäten haben Unternehmen zwei grundlegende Möglichkeiten: die Entwicklung einer firmeninternen Lösung oder den Kauf einer Enterprise-Lösung von einem Anbieter, der sich auf CIAM spezialisiert hat.

Wie ausführlich im Whitepaper Selbst entwickeln oder kaufen? Ein Leitfaden für CIAM (Customer Identity and Access Management) beschrieben, sind cloudbasierte, kommerzielle Standardlösungen in der Regel besser für die Ziele, Anforderungen und Ressourcen der meisten Unternehmen geeignet.[9] Dies gilt insbesondere für die Implementierung sowie für den Aufwand, der für den langfristigen Betrieb und die laufende Wartung einer Lösung erforderlich ist. Doch die Anforderungen von

Von der fortlaufenden Forschung und Entwicklung bis hin zu garantierten SLAs haben kommerzielle CIAM-Lösungen im Vergleich zu internen IT-Abteilungen mehrere entscheidende Vorteile. Cloud-Lösungen bieten flexible Skalierung, überregionale Failover und Disaster Recovery sowie ein Maß an Sicherheit, das mit internen Teams nur schwer zu erreichen ist.

Technologien, Verbrauchern, Märkten und Regulierungsbehörden ändern sich ständig. Insbesondere die neuesten Klauseln gesetzlicher Bestimmungen wie der DSGVO werden am besten von professionellen Lösungen Dritter erfüllt.

Kommerzielle CIAM-Lösungen bieten einige deutliche Vorteile gegenüber in der internen IT-Abteilung entwickelten Lösungen. Von globaler Verfügbarkeit und Skalierbarkeit bis hin zu garantierten Service-Level Agreements (SLAs) und Sicherheitszertifizierungen – dank der Kompetenz, der Ressourcen und der kontinuierlichen Forschungs- und Entwicklungsarbeit von Drittanbietern kann sich das interne IT-Team auf andere wichtige Geschäftsinitiativen konzentrieren.

CIAM-Lösungen, die die Möglichkeiten moderner Clouds für die gemeinsame Ressourcennutzung, flexible Skalierung, optimale Sicherheit sowie für überregionale Failover und Disaster Recovery nutzen, bieten umfassende IDaaS-Funktionen (Identity-as-a-Service) sowie ein Sicherheitsniveau, wie es mit intern entwickelten Produkten kaum zu erreichen ist. Gleichzeitig sorgen sie dafür, dass der Betrieb eigener Rechenzentren und Hardware verzichtbar wird.

Auch wenn der Aufbau eines eigenen Identitätsmanagementsystems machbar erscheint, besteht ein erhebliches Risiko, dass der Aufwand unterschätzt wird, zu wenig Finanzmittel bereitgestellt werden und langfristig nicht genügend interne Ressourcen und Fachkenntnisse vorhanden sind, um die Lösung zu unterstützen und zu warten sowie im Hinblick auf sich ändernde Marktanforderungen und Kundenerwartungen weiterzuentwickeln.

Kommerzielle CIAM-Anbieter können mit den von Technologien, Verbrauchern, Märkten und Regulierungsbehörden vorgegebenen Änderungen eher Schritt halten – denn Lösungsanbieter sind ganz einfach dazu gezwungen, ihre Services weiterzuentwickeln, damit ihre Angebote wettbewerbsfähig und relevant bleiben und die Compliance gewährleistet ist. Und da sie ihre Lösungen nicht nur für einen, sondern für viele Kunden entwickeln, bieten sich hier Vorteile, die bei der internen Lösungsentwicklung einfach nicht möglich sind.

Globales Pharmaunternehmen implementiert sichere Identitätsmanagement-Lösung, um Gesundheitsdienstleister zu unterstützen

Die Herausforderung

Ein führendes Pharmaunternehmen arbeitet mit Gesundheitsdienstleistern, Behörden und Gemeinden vor Ort zusammen, um den Zugang zu einer zuverlässigen und erschwinglichen Gesundheitsversorgung weltweit zu unterstützen und zu verbessern. Verschiedene Compliance-Bestimmungen zur Werbung für Produkte und Services bei Gesundheitsdienstleistern haben jedoch das Ziel des Unternehmens beeinträchtigt, Therapien schnell auf den Markt zu bringen. Das Unternehmen benötigte eine Identitätsmanagement-Lösung, mit der Gesundheitsdienstleister problemlosen und sicheren Zugriff auf die professionelle Unternehmens-Website erhalten, um Angebote für verschreibungspflichtige Medikamente zu nutzen. Dabei sollte die Website den landesspezifischen Vorschriften entsprechen. Um diese Anforderungen zu erfüllen, benötigte das Unternehmen eine professionelle CIAM-Lösung.

Die Lösung

Das Unternehmen entschied sich für Akamai Identity Cloud, um eine sichere Registrierungslösung im Corporate Design für seine professionelle Website zu implementieren, einschließlich Anmeldeworkflows, Single Sign-on, Authentifizierung, Passwortverwaltung, Kontoerstellung, Feldvalidierung und vielem mehr. Mit Profilverwaltungsfunktionen können Profilinformationen einfach bearbeitet werden, während die Profildatenspeicherung die Daten der Gesundheitsdienstleister automatisch in einer flexiblen, einheitlichen Cloud-Datenbank sammelt und speichert.

Die Identity Cloud-Plattform ist neunmal schneller als die vorherige Lösung des Unternehmens. Mit der Identity Cloud erhalten Gesundheitsdienstleister weltweit sicheren und einheitlichen Zugang zu regulierten medizinischen Ressourcen, während gleichzeitig geografisch unterschiedliche Sicherheits- und Compliance-Standards eingehalten werden. Gesundheitsdienstleister können Arzneimittelproben innerhalb von Tagen statt Wochen online über die sichere Website erhalten, wodurch die Patientenversorgung und die Lebensqualität der Patienten verbessert werden können. Die Mitarbeiter des Unternehmens konnten so ihre Produktivität steigern, da weniger Besuche bei Gesundheitsdienstleistern erforderlich sind, um Medikamentenproben und andere Ressourcen zu beziehen.

Darüber hinaus konnte das Pharmaunternehmen durch die Integration von Identity Cloud in die bestehenden Marketing-Technologieplattformen seine Marketingbemühungen bei Gesundheitsdienstleistern weltweit personalisieren.

Akamai Identity Cloud

Identity Cloud ist die CIAM-Lösung von Akamai. Die Plattform bietet alles, was Unternehmen benötigen, um ihren Kunden die Erstellung persönlicher Konten und die sichere Anmeldung auf Websites, in Apps und in IoT-basierten Anwendungen zu ermöglichen. Identity Cloud bietet Tools, mit denen der Aufwand für die Einhaltung der Datenschutzbestimmungen deutlich reduziert werden kann, während Unternehmen gleichzeitig ein hochsicheres Kundenprofil-Repository und eine 360-Grad-Sicht auf den Kunden erhalten.

Identity Cloud bietet spezifische Funktionen und Nutzererlebnisse, die Unternehmen bei der Erfüllung von Sicherheits- und gesetzlicher Anforderungen unterstützen. Identity Cloud umfasst Kundenregistrierung, Anmeldung, Authentifizierung, Single Sign-on, bereichsbezogene Zugriffskontrolle und das Einstellungs- und Zustimmungsmanagement sowie weitere Funktionen, mit denen personenbezogene Daten gesammelt, verwaltet und gesichert werden.

Durch die Implementierung von Identity Cloud können Unternehmen und Organisationen ein unternehmensweites Identitätsmanagement auf schnelle und flexible Weise implementieren. Die Lösung wurde mit einer cloudnativen Architektur entwickelt und wird automatisch je nach Kapazitätsanforderungen skaliert. So bewältigt die Lösung hohen Traffic und bietet die nötige Skalierbarkeit für Hunderte Millionen von Nutzern sowie die Sicherheit, Performance und Verfügbarkeit, die für die Bereitstellung geschäftskritischer Anwendungen erforderlich sind. Akamai Identity Cloud wurde dafür konzipiert, Unternehmen bei der Einhaltung internationaler Sicherheits- und Datenschutzbestimmungen zu unterstützen, das Vertrauen in ihre Marke zu stärken, Kundendaten zu verwalten und Risiken zu minimieren, indem die Daten in allen Regionen und Anwendungen sicher verfügbar gemacht werden.

Fazit

Neben den immer strengeren Datenschutzbestimmungen sind die Sicherheit und der Datenschutz von Kundenidentitäten für Unternehmen, die enge und vertrauenswürdige digitale Beziehungen zu ihren Kunden aufbauen möchten, von entscheidender Bedeutung. Verbraucher haben immer höhere Erwartungen an die vertrauliche und sichere Aufbewahrung ihrer personenbezogenen Daten. Die vielen Fälle von Datenmissbrauch, Sicherheitsverstößen und Identitätsdiebstahl in den Schlagzeilen haben die Messlatte für Unternehmen höher gelegt, um als vertrauenswürdiger Verwalter personenbezogener Daten angesehen zu werden. Wenn Kunden ihre Daten bei einem Unternehmen speichern, gehen sie damit einen Vertrauensvertrag ein. Wenn dieses Vertrauen verletzt wird, ist es in der Regel sehr schwierig, es wiederherzustellen.

QUELLEN

1) EU-Datenschutzvorschriften, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_de
2) Gesetzliche Vorschriften in Kalifornien: AB-375 Privacy, https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
3) Personal Information Protection and Electronic Documents Act (PIPEDA), https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
4) IBM-Bericht „Cost of a Data Breach" (Kosten durch Datendiebstahl) aus dem Jahr 2019, https://www.ibm.com/security/data-breach
5) Akamai-Whitepaper: DSGVO, CCPA und andere Vorschriften zum Datenschutz: Wie Unternehmen mithilfe von Identity Governance das Vertrauen ihrer Kunden wahren und erhöhen https://www.akamai.com/de/de/multimedia/documents/white-paper/gdpr-ccpa-and-beyond-white-paper.pdf
6) Davis Wright Tremaine: CCPA-Nachahmungsgesetze in Bundesstaaten im ganzen Land eingeführt, https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) ZDNet: Marriott aufgrund des Datenschutzvorfalls im letzten Jahr in Großbritannien zu 123 Million US-Dollar DSGVO-Geldstrafe verurteilt, 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): So führen Sie eine Datenschutz-Folgenabschätzung durch, https://gdpr.eu/data-protection-impact-assessment-template/
9) Akamai-Whitepaper: Selbst entwickeln oder kaufen? Ein Leitfaden für CIAM (Customer Identity and Access Management), https://www.akamai.com/de/de/multimedia/documents/white-paper/build-vs-buy-a-guide-for-customer-identity-and-access-management.pdf

Akamai

Akamai stellt sichere digitale Erlebnisse für die größten Unternehmen der Welt bereit. Die Intelligent Edge Platform umgibt alles – vom Unternehmen bis zur Cloud –, damit unsere Kunden und ihre Unternehmen schnell, intelligent und sicher agieren können. Führende Marken weltweit setzen auf die agilen Lösungen von Akamai, um die Performance ihrer Multi-Cloud-Architekturen zu optimieren. Akamai bietet Schutz vor Angriffen und Bedrohungen, beschleunigt Entscheidungen und Anwendungen und liefert herausragende Online-Erlebnisse. Das Akamai-Portfolio für Website- und Anwendungsperformance, Cloudsicherheit, Unternehmenszugriff und Videobereitstellung wird durch einen herausragenden Kundenservice, Analysen und Rund-um-die-Uhr-Überwachung ergänzt. Warum weltweit führende Unternehmen auf Akamai vertrauen, erfahren Sie unter www.akamai.com, im Blog blogs.akamai.com oder auf Twitter unter @Akamai. Unsere globalen Standorte finden Sie unter www.akamai.com/locations. Veröffentlicht: November 2019.