Wie eine moderne DLP-Lösung die Umsetzung der DSGVO unterstützt

Die seit 2018 geltende Datenschutz-Grundverordnung (DSGVO) ist die Reaktion der europäischen Gesetzgeber auf die technologischen Fortschritte der letzten 20 Jahre. Das weitreichende Regelwerk soll allen in der EU ansässigen Personen mehr Kontrolle über die Erfassung und Verarbeitung ihrer personenbezogenen Daten verschaffen und gewährt ihnen zu diesem Zweck unter anderem das Recht auf Auskunft, Berichtigung und Löschung („Recht auf Vergessenwerden“) sowie auf Datenübertragbarkeit.

Dabei ist aus unternehmerischer Sicht zunächst einmal beachtenswert, dass die DSGVO für alle Körperschaften gilt, die für personenbezogene Daten von in der EU befindlichen Personen verantwortlich sind oder solche Daten verarbeiten. Außerdem wird der Begriff „personenbezogene Daten“ in der Verordnung relativ weit gefasst und bezeichnet dort alle Informationen, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen. Dazu zählen zum einen der Name, die E-Mail-Adresse und das Geburtsdatum, die Telefonnummer oder Benutzer-ID, zum anderen solche Angaben, die ein potenziell von einer Einzelperson benutztes Gerät identifizieren, wie z. B. die IP-Adresse, anhand derer sich die Online-Aktivitäten einer Person verfolgen und ihre Standortdaten ermitteln lassen. Zugleich ist zu betonen, dass die DSGVO nicht nur für in der EU ansässige Unternehmen, sondern auch für außerhalb der Europäischen Union niedergelassene Firmen gilt, sofern sie EU-Bürgern und -Einwohnern Waren und Dienstleistungen anbieten oder das Verhalten von EU-Bürgern und -Einwohnern in der EU beobachten. Das bedeutet in der Praxis, dass jeder in der EU operierende Service-Anbieter zur Umsetzung und Einhaltung der DSGVO verpflichtet ist, sofern er personenbezogene Daten erfasst oder verarbeitet.

Grundsätzlich müssen die der DSGVO unterliegenden Unternehmen Prozesse und Sicherheitstools implementieren, mit denen sie die gesetzeskonforme Handhabung und den kontinuierlichen Schutz der personenbezogenen Daten von in der EU ansässigen Personen sicherstellen und die Speicherorte dieser Daten jederzeit ermitteln können. Werden diese Vorgaben nicht dauerhaft umgesetzt, drohen empfindliche Bußgelder, schwerwiegende Imageschäden und mögliche Schadenersatzklagen von Betroffenen.

Daher sind die verantwortlichen Manager aufgefordert, Datensicherheit und Datenschutz durch entsprechende Initiativen zu stärken (und so auch die Weichen für die Umsetzung ähnlicher gesetzlicher Regelungen in anderen Ländern und Regionen zu stellen). Allerdings kommt die Umsetzung konkreter Maßnahmen in vielen Unternehmen trotz des enormen Handlungsdrucks weiterhin nur schleppend voran, weil die nötigen Einblicke fehlen und die Complianceprozesse auf manuellen Abläufen basieren. Erschwerend kommt hinzu, dass personenbezogene Informationen immer vielfältigere Formen annehmen und auf immer mehr Standorte verteilt sind. In Anbetracht dessen scheint die Zeit reif für Investitionen in neue Technologien, die den zuständigen Teams das Compliance- und Risikomanagement, die Umsetzung von Best Practices zur Stärkung der Datensicherheit, die lückenlose Überwachung der Datennutzung und der Speicherorte sowie die Erkennung von Sicherheitsverletzungen und die Erstellung von Notfallplänen erleichtern.

Der mangelnde Überblick über die eigenen Datenbestände

Wie bereits erwähnt, nimmt die DSGVO moderne Unternehmen in die Pflicht, ihre Maßnahmen zur Sicherung persönlicher und personenbezogener Daten zu verbessern. Dabei besteht die größte Herausforderung darin, dass die vielfältigen gesetzlich geschützten Informationen an einer ständig wachsenden Zahl von Standorten erfasst, aufbewahrt und abgerufen werden.

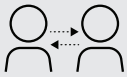
Zum einen steigt im Zuge der fortgesetzten Migration in die Cloud das Volumen der in SaaS-Anwendungen und auf privaten oder öffentlichen Cloud-Plattformen gespeicherten sensiblen Daten – und damit auch die Wahrscheinlichkeit fahrlässiger Datenschutzverletzungen. Zum anderen vervielfacht der ungebrochene Trend zur mobilen Arbeit die Zahl der Remotestandorte, an denen personenbezogene Informationen und andere sensible Daten weniger stark geschützt sind und daher unabsichtlich in falsche Hände gelangen können.

Drei Handlungsschwerpunkte

Angesichts dieser umfangreichen Herausforderungen stellen sich viele CISOs und InfoSec-Manager die Frage, wo sie mit ihren Datenschutz- und Compliance-Initiativen ansetzen können. Aus unserer Sicht gibt es hier drei Handlungsschwerpunkte, auf die sich Sicherheitsexperten bei der Erstellung eines Datenschutzframeworks zur Umsetzung der DSGVO konzentrieren sollten. Im Einzelnen handelt es sich dabei um die folgenden Bereiche:

1. **Identifizierung der gesetzlich zu schützenden Datenbestände**: Erforderlich ist eine genaue Aufstellung aller Datenbestände, die personenbezogene Informationen zu in der EU ansässigen Personen enthalten.
2. **Prävention von Datenlecks**: Die der DSGVO unterliegenden Unternehmen müssen alle sensiblen personenbezogenen Daten durch geeignete Maßnahmen vor externen Bedrohungen, böswilligen Insidern und der fahrlässigen Offenlegung durch unachtsame Mitarbeiter schützen. Das ist nicht zuletzt deshalb angeraten, weil die Verantwortlichen im Fall von Datenlecks und Datenschutzverletzungen verpflichtet sind, sowohl die zuständigen Regulierungsbehörden als auch die betroffenen Personen innerhalb festgesetzter Fristen zu benachrichtigen. Erfolgt die Meldung nicht rechtzeitig, drohen Sammelklagen, Schadenersatzforderungen und Imageschäden.
3. **Implementierung der erforderlichen Prozesse und Tools**: Die DSGVO gewährt Kunden das Recht, von Unternehmen Auskunft über alle gespeicherten Daten zu ihrer Person sowie die Löschung dieser Informationen zu verlangen (wobei gewisse Ausnahmen gelten). Deshalb müssen die Verantwortlichen jederzeit ermitteln können, wo die entsprechenden Daten gespeichert sind. Außerdem empfiehlt sich der Einsatz von Überwachungstools, mit denen sich die Übertragung personenbezogener Daten verfolgen lässt, sowie die Implementierung von Zero-Trust-Zugangskontrollen, Least-Privilege-Zugriffsrechten und starken Datensicherheitsmaßnahmen.

Empfehlungen



Stoßen Sie den Dialog mit dem Vorstand an und erstatten Sie über den Fortschritt Ihrer Datenschutzinitiative Bericht

Identifizieren Sie die größten Risiken in Sachen Datenschutz und Datensicherheit

Ermitteln Sie, welche personenbezogenen Daten in Ihrem Unternehmen gespeichert werden, und stellen Sie die Rechtmäßigkeit der Datennutzung sicher

Unterstützen Sie die Umsetzung der DSGVO durch geeignete Technologien

Abbildung 1: DSGVO-Compliance in vier Schritten

Ein umfassender Ansatz für Datensicherheit und Datenschutz

DSGVO-Compliance lässt sich nicht durch punktuelle Maßnahmen erreichen. Stattdessen bedarf es einer umfassenden, konsolidierten Datensicherheitsstrategie, die die gesamte Netzwerkinfrastruktur, sämtliche On-Premises- und Cloud-Umgebungen sowie alle mobilen Benutzer abdeckt – und den Verantwortlichen die Bewältigung der folgenden Herausforderungen ermöglicht:

- Identifizierung von Datenbeständen mit personenbezogenen Informationen und Überwachung der Speicherung und Übertragung dieser Daten
- Implementierung von Datensicherheitsmechanismen zur Unterbindung des Zugriffs durch Unbefugte
- Prävention von Datenlecks und Datensicherheitsverletzungen
- Zeitnahe Reaktion auf akute Vorfälle

Dabei resultiert die erste hier aufgeführte Herausforderung aus der Tatsache, dass personenbezogene Daten nicht nur im eigenen Rechenzentrum bzw. in privaten Clouds, sondern auch auf geschäftlich genutzten IT-Geräten, SaaS-Anwendungen und Public-Cloud-Plattformen erfasst und gespeichert werden. Außerdem findet die Übertragung dieser sensiblen Informationen über verschiedenste Kanäle statt, darunter verschlüsselte und unverschlüsselte Internetverbindungen, Filesharing-Apps, cloudbasierte Speicherlösungen und Mobilfunknetze. Deshalb stellt sich die Frage: **Wie lässt sich ermitteln, wo personenbezogene Daten gespeichert sind und wie sie übertragen werden?**

Die zweite Herausforderung verweist auf das Risiko von Datenlecks durch Fehlverhalten der Mitarbeiter. So kann es zum einen vorkommen, dass wohlmeinende Angestellte ungenehmigte SaaS-Anwendungen oder Cloud-Repositorys zur Übertragung oder Speicherung sensibler Daten nutzen oder personenbezogene Informationen in fahrlässiger Weise an nicht vertrauenswürdige Dritte senden. Zum anderen sind immer wieder Datendiebstähle durch böswillige Insider zu beobachten. Das wirft die Frage auf: **Wie lässt sich sicherstellen, dass personenbezogene Daten nicht versehentlich offengelegt werden und nur für autorisierte Benutzer zugänglich sind?**

Drittens ist unmittelbar einsichtig, dass Datenlecks und Datensicherheitsverletzungen vermieden werden sollten, weil sie gravierende Auswirkungen für die betroffenen Unternehmen haben können. Aus diesem Grund müssen die Verantwortlichen in der Lage sein, sowohl emailbasierte Phishing- und Malware-Angriffe und schädliche Dateidownloads als auch unabsichtliche Datenlecks durch befugte Benutzer zu verhindern. Vor allem aber müssen die personenbezogenen Daten auch dann jederzeit geschützt sein, wenn sie aus gesetzlich zulässigen Gründen an einen Partner oder Drittanbieter übermittelt werden. Dies führt zu der schwierigen Frage: **Wie können Datenlecks und Datensicherheitsverletzungen jenseits des eigenen Netzwerks verhindert und unterbunden werden?**

Was nun die vierte und letzte Herausforderung angeht, so ergibt sich diese aus den in der DSGVO festgelegten Melde- und Benachrichtigungspflichten. Hier stehen die Verantwortlichen vor der Frage: **Wie lässt sich sicherstellen, dass die Untersuchung und Behebung eines akuten Vorfalls innerhalb der festgesetzten Fristen abgeschlossen werden kann?**

Unternehmenstaugliche DLP-Lösungen als DSGVO-Compliancetools

Moderne, branchenführende DLP-Technologien wurden speziell für die automatische Identifizierung, Überwachung und Sicherung aller sensiblen Daten im Zuständigkeitsbereich eines Unternehmens konzipiert. Sie erleichtern die konsequente Umsetzung der DSGVO und anderer gesetzlicher Vorgaben, weil sie über kontextsensitive Funktionen für die automatische Erkennung personenbezogener Daten und vorkonfigurierte Regeln für alle relevanten Verordnungen verfügen. Dabei profitieren Kunden von verkürzten Konfigurations- und Anpassungsprozessen.

Vor allem aber beseitigt eine moderne DLP-Lösung blinde Flecken und Probleme rund um die Schatten-IT, indem sie einen lückenlosen Überblick über den gesamten Traffic im Unternehmensnetzwerk sowie den Datenverkehr aller mobilen Arbeiter, genehmigten und nicht genehmigten Cloud-Apps und cloudbasierten Repositorys bietet. Das hilft den Verantwortlichen im Unternehmen, sämtliche Zugriffe auf sensible Daten zu überwachen und jede missbräuchliche Nutzung umgehend aufzudecken. Außerdem unterstützt die Technologie in Kombination mit anderen Sicherheitstools – beispielsweise für die Benutzerauthentifizierung, Daten-Governance und das Berechtigungsmanagement – die Umsetzung des Modells der minimalen Zugriffsrechte und die Implementierung sicherer Datenaustauschprozesse mit Dritten. Zusätzlich kann eine moderne DLP-Lösung einen entscheidenden Beitrag zur automatischen Unterbindung von Richtlinienverstößen leisten, indem sie Benutzer vor nicht konformen Aktivitäten warnt, unsichere Datenübertagungen stoppt, sensible Informationen schwärzt und verschlüsselt und die Weitergabe oder Offenlegung vertraulicher Daten über SaaS-Anwendungen einschränkt.

Zusammengenommen bieten die genannten Features und Funktionen also beträchtliche Vorteile, wenn es um die Umsetzung der in der DSGVO enthaltenen Datenschutzvorgaben geht. Daher sind entsprechende Investitionen dringend angeraten: **DLP-Technologien der neuesten Generation versetzen Unternehmen in die Lage, ihre ambitionierten Ziele in Sachen Datensicherheit zu erreichen und strenge Regularien erfolgreich zu implementieren.**

Im Gegensatz dazu erweisen sich konventionelle DLP-Lösungen als defizitär, da sie im Laufe der Jahre allzu komplex geworden sind, in der On-Premises-Infrastruktur gehostet werden müssen und sich nur mit hohem Kostenaufwand um neue Funktionen und Features erweitern lassen. Ähnliches gilt für neuere Produkte mit integrierten DLP-Funktionen, die meist lediglich einen Teil der Umgebungen und Benutzer abdecken. Angesichts dessen setzt sich in den Führungsetagen zunehmend die Erkenntnis durch, dass eine moderne DLP-Lösung der Enterprise-Klasse mit physischen und cloudbasierten Sicherheitspunkten die einzige Möglichkeit ist, die aus der digitalen Transformation resultierenden Datensicherheitsanforderungen zu bewältigen – zumal eine entsprechende Investition spürbare Vorteile in Sachen betriebliche Effizienz und Skalierbarkeit sowie sinkende Betriebskosten verspricht. Nicht umsonst äußerten in einer aktuellen Studie der ESG 40 Prozent der Befragten die Erwartung, den Umstieg auf cloudbasierte Netzwerksicherheitslösungen binnen zwei Jahren abschließen zu können.[1]

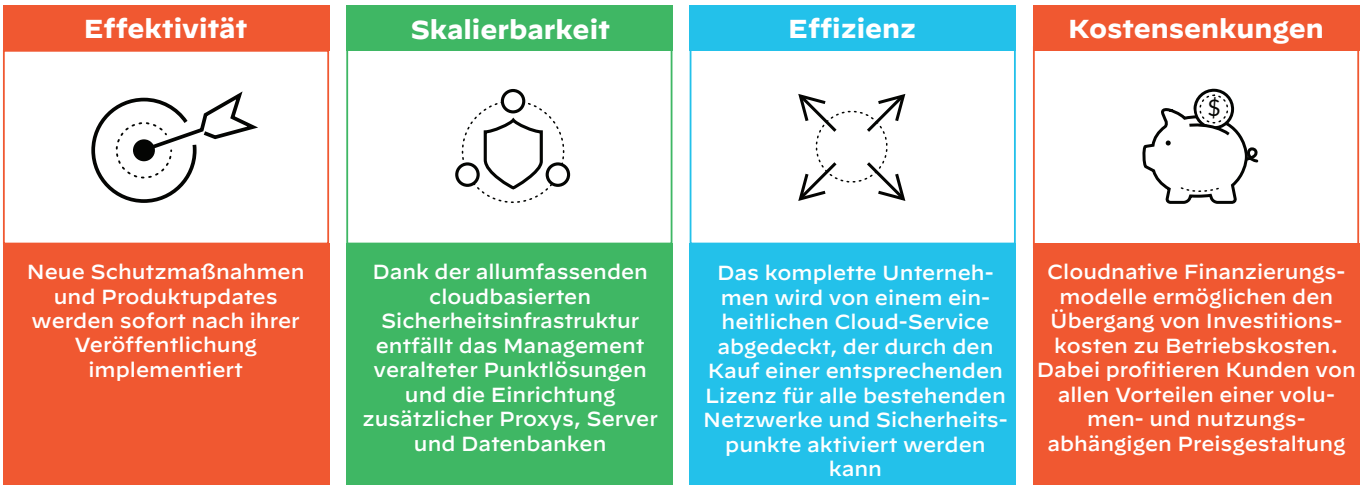


Abbildung 2: Wichtige Vorteile einer modernen, cloudbasierten DLP-Lösung

Enterprise DLP von Palo Alto Networks

Enterprise DLP von Palo Alto Networks erleichtert modernen Unternehmen die Bewältigung der zahlreichen aktuellen Herausforderungen rund um die Datensicherheit und den Datenschutz in hochgradig verteilten Cloud- und Hybrid-Infrastrukturen. Die innovative, cloudbasierte Lösung stellt vielfältige automatische Funktionen für die Erkennung, Überwachung und Abschirmung sensibler Daten und personenbezogener Informationen bereit und überwindet damit die Defizite älterer Datensicherheitstechnologien.

Nach dem Umstieg profitieren Kunden unter anderem von vordefinierten, bis ins Detail individuell anpassbaren Erfassungsregeln und Kontextbedingungen, die eine extrem zuverlässige Erkennung sensibler Daten im Sinne der DSGVO sicherstellen. Damit lassen sich Konfigurations- und Anpassungsprozesse automatisieren und spürbar beschleunigen.

Zusätzlich erleichtert die funktionsreichste cloudbasierte DLP-Lösung der Branche die Vermeidung von blinden Flecken und lästigen Problemen in puncto Schatten-IT, indem sie einen lückenlosen Überblick über den Datenverkehr aller mobilen Mitarbeiter, Unternehmensfilialen sowie SaaS-, IaaS- und PaaS-Lösungen bietet. Dabei müssen unternehmensweite DSGVO-Richtlinien nur einmal definiert werden, da die Implementierung in allen On-Premises- und Cloud-Umgebungen synchron und automatisiert durch unseren Dienst erfolgt. So können die Verantwortlichen alle Infrastrukturen und Benutzer konsistent überwachen und unnötige manuelle Erstellungsprozesse im Rahmen von Erweiterungsprojekten vermeiden.

Und da unser neuer DLP-Service von Haus aus für die Integration mit unseren ML-gestützten – physischen, virtuellen und cloudbasierten – Next-Generation Firewalls und den Cloud-Sicherheitsprodukten der Prisma®-Suite ausgelegt ist, können Kundenunternehmen auch bei der Übertragung sensibler Daten in physischen und virtuellen Netzwerken und Cloud-Umgebungen sowie bei der Aufbewahrung personenbezogener Informationen in SaaS-Apps und auf cloudnativen IaaS-Plattformen für einen effektiven Inlineschutz aller Benutzer sorgen – und zwar unabhängig davon, ob deren Geräte in eine Campus- oder Filialinfrastruktur eingebunden sind oder für mobile Arbeit genutzt werden. Als Basis dienen auch hier die bereits angesprochenen DSGVO-Richtlinien, anhand derer die Lösung die Verarbeitung und Übertragung gesetzlich geschützter Daten identifiziert und automatisch auf nicht konforme Aktivitäten, Speicherorte und Datendiebstahlsversuche prüft.

1. „Transitioning Network Security Controls to the Cloud“, ESG, August 2020, https://www.esg-global.com/research/esg-research-report-transitioning-network-security-controls-to-the-cloud.

Abgesehen davon eröffnen sich den Verantwortlichen neue Einsparmöglichkeiten, da die einfach zu implementierende, benutzerfreundliche und pflegeleichte DLP-Lösung von Palo Alto Networks die Installation zusätzlicher Softwarelösungen, Proxys, Server, Datenbanken, Cloud-Konnektoren und IT-Ressourcen überflüssig macht und damit in Bezug auf die Gesamtbetriebskosten dreimal günstiger ist als konventionelle DLP-Technologien.

Zugleich sollte jedoch nicht vergessen werden, dass eine Technologie allein nicht ausreicht, um die vielfältigen Anforderungen in Sachen Datenschutz-Compliance umzusetzen. Zum Schutz sämtlicher Netzwerke, Endpunkte, Clouds und Benutzer empfehlen wir einen mehrschichtigen Sicherheitsansatz.

Fazit

Wenn Sie nach neuen Möglichkeiten suchen, die immer strengeren gesetzlichen Datensicherheits- und Datenschutzanforderungen umzusetzen, sollten Sie unbedingt die Implementierung einer cloudbasierten DLP-Lösung im Rahmen einer umfassenden, ganzheitlichen Strategie in Erwägung ziehen. Weitere Informationen zu diesem Thema finden Sie auf unserer Website.

paloalto NETWORKS

Oval Tower, De Entrée 99–197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 7239771
Support: +31 20 808 4600

www.paloaltonetworks.de