ManageEngine
EventLog Analyzer

Alles, was Sie bezüglich der Einhaltung der Datenschutz-Grundverordnung der EU wissen und tun müssen

Inhalt

Einleitung 2

Herausforderungen, Anforderungen und Maßnahmenpläne

DSGVO ist grenzenlos 3

Eine breitere Definition für persönliche Daten 4

Neudefinition von Datenschutzprinzipien 5

Zuständigkeiten und Rechenschaftspflichten 7

Benachrichtigungen über Datenschutzverletzungen 9

Die Rechte von Datensubjekten 10

Strafen bei Compliance-Verstößen 11

Über EventLog Analyzer 12

EventLog Analyzer und seine Rolle bei der Erfüllung der DSGVO-Vorgaben 13

Einführung

Die wachsende Anzahl, der immer größere Umfang und die immer höheren Kosten von Datenschutzverletzungen haben dazu geführt, dass Regierungen auf der ganzen Welt nun strenge Compliance-Gesetze zum Schutz der persönlichen Daten ihrer Bürger einführen. Auch Europa ist keine Ausnahme. Seit 2012 entwirft die EU-Kommission neue Datenschutzregeln, die Datenverarbeitungsmethoden verbessern, die Datensicherheit erhöhen und den Schutz empfindlicher Daten in allen europäischen Ländern harmonisieren können.

Angesichts der vielen Änderungen an den bestehenden Datenschutzrichtlinien erlangt die neue Datenschutz-Grundverordnung (DSGVO) immer mehr Aufmerksamkeit. Die Umsetzung des DSGVO-Rahmenwerks der EU gestaltet sich komplex, da neue Richtlinien für die Rechenschaftspflicht, neue Verfahren bei Datenschutzverletzungsmeldungen und strengere Regeln für internationale Datenflüsse zu berücksichtigen sind. Da nur noch wenige Monate verbleiben, um die Anforderungen der neuen Verordnung zu erfüllen, ist es für viele Unternehmen an der Zeit, ihre Sicherheitsstrategien zu überdenken.

Dieses Handbuch erläutert die wichtigsten Veränderungen, Herausforderungen und Maßnahmenpläne, mit denen sich Unternehmen befassen sollten, um die Einhaltung der DSGVO zu gewährleisten.

Veränderungen, Anforderungen und Maßnahmenpläne

DSGVO ist grenzenlos

Die DSGVO ist ein globales Datenschutzgesetz, das über allein in der EU aktive Unternehmen hinausgeht. Alle Unternehmen, die Verbraucher in der EU ansprechen, die persönlichen Daten von EU-Bürgern verarbeiten oder das Verhalten von EU-Datensubjekten überwachen, müssen die Anforderungen der DSGVO erfüllen.

Anforderungen:

- Es wird Zeit, die Sicherheitsstrategien und Richtlinien von Unternehmen zu überprüfen. Unternehmen, die nicht innerhalb der EU agieren, aber mit EU-Daten arbeiten, müssen die erforderlichen Maßnahmen ergreifen, um DSGVO-Konformität zu gewährleisten.
- Unternehmen, die innerhalb der EU agieren und die Anforderungen des bestehenden EU-Datenschutzgesetzes erfüllen, sollten ihre Sicherheitsstrategie ebenfalls überprüfen, um sicherzustellen, dass diese die stringenten Anforderungen der neuen DSGVO erfüllt.

Die Maßnahmenpläne

- Wenn Ihr Unternehmen Waren oder Dienstleistungen für EU-Bürger bereitstellt oder deren Verhalten überwacht, müssen Sie bis spätestens zum 25. Mai 2018 die Anforderungen der DSGVO erfüllen.
- Überprüfen Sie Ihre Sicherheitsrichtlinien und stellen Sie sicher, dass Sie bei der Handhabung persönlicher Daten die unten beschriebenen Maßnahmen ergreifen.
- Entwerfen Sie angemessene Datenschutzerklärungen und andere Dokumente, mit denen Sie die explizite und eindeutige Zustimmung von Personen zur Verarbeitung ihrer persönlichen Daten einholen können. Sollten Sie bereits derartige Dokumente besitzen, erwägen Sie eine Überprüfung und Überarbeitung im Hinblick auf die neuen Vorschriften.
- Überwachen Sie die technischen und organisatorischen Maßnahmen, die zur Gewährleistung der Privatsphäre und Sicherheit erhobener persönlicher Daten ergriffen werden.
- Falls nötig, ernennen Sie Beauftragte, die die Datenprozesse überwachen können und für die Sicherheit persönlicher und empfindlicher Daten verantwortlich sind.

Eine breitere Definition für persönliche Daten

Die neue Richtlinie weitet die Definition persönlicher Daten und empfindlicher persönlicher Daten aus.

Der DSGVO zufolge handelt es sich bei persönlichen Daten um „Informationen bezüglich einer identifizierten und identifizierbaren natürlichen Person“. Sie umfasst ebenfalls „Online-Identifikatoren“ wie IP-Adressen und Cookie-Identifikatoren.

Neben der Definition persönlicher Daten kategorisiert die DSGVO einige der persönlichen Daten als empfindliche persönliche Daten. Der DSGVO zufolge handelt es sich bei empfindlichen persönlichen Daten um „alle Daten, die die Rasse oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Zugehörigkeit zu einer Gewerkschaft, die Gesundheit oder das Sexualleben sowie genetische und biometrische Daten“ betreffen.

Die neuen Anforderungen setzen ebenfalls voraus, dass Unternehmen vor der Verarbeitung persönlicher Daten eine gültige Einwilligung von den „Datensubjekten“ erhalten.

Herausforderungen:

- Diese weite Definition persönlicher Daten und die Einbeziehung des „Online-Identifikators“ zwingt Unternehmen, die mit Datenanalytik, Verhaltensanalyse, Werbung und sozialen Medien arbeiten, die DSGVO-Anforderungen zu erfüllen.

Die Maßnahmenpläne

- Definieren Sie den Umfang der Daten, mit denen Ihr Unternehmen arbeitet.
- Wenn die Daten der DSGVO-Definition von „persönlichen Daten“ entsprechen, verfassen Sie eine Datenschutzerklärung oder ein Dokument, dass die explizite und eindeutige Einwilligung von Personen zur weiteren Datenverarbeitung anfordert.
- Sollten Sie diese Einwilligung zur Datenverarbeitung bereits anfordern, erwägen Sie deren Überprüfung und Überarbeitung im Hinblick auf die neuen Compliance-Vorschriften.

Neudefinition von Datenschutzprinzipien

Das Datenschutzprinzip, das den Rückgrat der DSGVO-Anforderungen bildet, ist mit dem des früheren Datenschutzgesetzes identisch. Dabei werden jedoch einige zusätzliche Elemente hinzugefügt.

Die sechs Datenschutzprinzipien geben vor, dass persönliche Daten und empfindliche persönliche Daten:

- nach Treu und Glauben, rechtmäßig und auf transparente Art und Weise verarbeitet werden müssen.
- für bestimmte, explizite und rechtmäßige Zwecke erhoben werden und nicht auf eine Art und Weise verarbeitet werden dürfen, die den obigen Zwecken widerspricht. Die weitere Archivierung von Daten im öffentlichen Interesse oder zu wissenschaftlichen, historischen oder statistischen Zwecken darf nicht im Widerspruch zu den ursprünglichen Zwecken stehen.
- ausreichend, relevant und auf das beschränkt sein müssen, das für den Verarbeitungszweck benötigt wird
- wahrheitsgemäß und aktuell sein müssen. Maßnahmen müssen ergriffen werden, um fehlerhafte Daten zu löschen oder zu überarbeiten.
- in einer Form aufbewahrt werden müssen, welche die Identifikation von Datensubjekten nicht länger ermöglicht, als für die Verarbeitungszwecke erforderlich. Sie dürfen nur für einen längeren Zeitraum aufbewahrt werden, wenn eine solche Archivierung im öffentlichen Interesse ist oder wissenschaftlichen, historischen oder statistischen Zwecken dient. Darüber hinaus müssen Unternehmen technische Maßnahmen ergreifen, um die Rechte und die Freiheit von Personen zu schützen.
- mit den geeigneten technischen und organisatorischen Maßnahmen verarbeitet werden, welche ein entsprechendes Maß an Sicherheit gewährleisten, darunter Schutz vor rechtswidriger Verarbeitung, unbeabsichtigtem Verlust, Zerstörung oder Beschädigung.

Die neue DSGVO gibt strenge Rechenschaftspflichten vor, nach denen Datenverantwortliche a) verantwortlich für die Umsetzung von Datenschutzprinzipien sind und b) nachweisen müssen, dass das Unternehmen die DSGVO-Anforderungen erfüllt.

Anforderungen:

- Neben der Erfüllung der Datenschutzprinzipien selbst müssen Unternehmen ihre Rolle bei der Datenverarbeitung definieren (d.h. Datenverantwortliche oder Datenverarbeiter) und ihre Rolle im Rahmen der neuen Vorschriften übernehmen.
- Unternehmen sollten ihre Daten-Audit-Flüsse überprüfen, um die neuen Anforderungen an die Rechenschaftspflicht der DSGVO zu erfüllen.

- Ein neuer, risikobasierter Ansatz sollte von Unternehmen übernommen werden, wenn diese persönliche Daten mit hohem Risiko verarbeiten. Datenverantwortliche müssen Datenschutzfolgeabschätzungen durchführen, um das mit den persönlichen Daten verbundene Risiko bereits vor der Verarbeitung einzustufen. Die DSGVO gestattet ebenfalls die Identifizierung und Minderung von Datenschutzverletzungen in einer frühen Phase, um mögliche Schäden einzugrenzen.
- Wenn ein Projekt, bei dem persönliche Daten erforderlich sind, initiiert wird, sollten sich Unternehmen an einem „Grundsatz des eingebauten Datenschutzes“ orientieren, um das Risiko von Datenschutzverletzungen zu minimieren.

Die Maßnahmenpläne

- Dokumentieren Sie alle für die Datenverarbeitung relevanten Informationen, darunter:
  - Welche Art von persönlichen Daten erhoben wird
  - Wie diese erhoben, verwendet, übertragen und gespeichert werden.
  - Wie diese bei jedem Schritt vor der Offenlegung geschützt werden.
- Neben der Dokumentation von Informationen, darunter Speicherort und Besitzer der Daten, sollten Unternehmen ebenfalls folgende Aktivitäten ständig überwachen:
  - Wer auf persönliche Daten zugreift.
  - Mit wem die Daten geteilt werden.
- Überwachen Sie die Datei oder den Ordner, in der bzw. dem Daten gespeichert werden, ständig. So können Sie jegliche unbefugten oder illegalen Zugriffsversuche sofort identifizieren und melden.
- Führen Sie Unterlagen dazu, wie lange die Daten gespeichert werden sollen. Und stellen Sie beim Speichern der Daten sicher, dass diese verschlüsselt und nicht manipulierbar sind.

Zuständigkeit und Rechenschaftspflicht

Jedes Unternehmen, das persönliche oder empfindliche Daten verarbeitet, agiert entweder als Verarbeiter oder als Verantwortlicher. Zur Gewährleistung der Rechenschaftspflicht schafft die DSGVO ein Gleichgewicht zwischen den Rollen des Verarbeiters und des Verantwortlichen. Damit sind diese gleichermaßen für die Einhaltung der Anforderungen verantwortlich.

Datenverantwortliche

- Der DSGVO zufolge sind „Verantwortliche jede juristische Person, die entweder allein oder gemeinsam mit anderen bestimmt, wie und warum persönliche Daten verarbeitet werden“.
- Verantwortliche sind verantwortlich für:
  - die Überprüfung aller Datenverarbeitungsaktivitäten.
  - die Führung relevanter Unterlagen zu allen Datenverarbeitungsaktivitäten.
  - die Durchführung von Datenschutzrisikobewertungen bei risikoträchtigen Prozessen.
  - die Implementierung des eingebauten, standardmäßigen Datenschutzes.
  - die Ernennung von Datenverarbeitern und die Definition von Anweisungen zur Datenverarbeitung.
  - die Benachrichtigung von Behörden bei Datenschutzverletzungen.

Datenverarbeiter

- Der DSGVO zufolge sind Datenverarbeiter „eine Person (außer den Mitarbeitern des Datenverantwortlichen), die Daten im Auftrag des Datenverantwortlichen verarbeitet“.

  Datenverarbeiter tun Folgendes:

  - Sie verarbeiten Daten nur auf dokumentierte Anweisung des Verantwortlichen.
  - Sie implementieren Sicherheits- und Organisationsmaßnahmen, um Datenschutzverletzungen zu vermeiden.
  - Sie löschen sämtliche persönliche Daten nach der Verarbeitung und auf Anweisung des Verantwortlichen.
  - Sie führen Buch über Verarbeitungsaktivitäten, die im Auftrag der Verantwortlichen durchgeführt werden.
  - Sie ernennen falls erforderlich einen Datenschutzbeauftragten.
  - Sie benachrichtigen die Verantwortlichen umgehend im Falle einer Datenschutzverletzung.
  - Sie stellen den Verantwortlichen sämtliche Informationen zur Verfügung zu, die zum Nachweis der Compliance nötig sind und gestatten von den Verantwortlichen durchgeführte Audits.

Anforderungen:

- Unternehmen sollten ihre bestehenden Datenverarbeitungsvereinbarung sorgfältig überprüfen und überarbeiten, um auf die neuen Anforderungen zur Rechenschaftspflicht zu reagieren. Sämtliche neue Vereinbarungen müssen berücksichtigen: die neuen DSGVO-Anforderungen.
- Sowohl Verarbeiter als auch Verantwortliche sollten ihre Sicherheits-, Auditing-, und Datenschutzverletzungsrichtlinien überprüfen und sie an die neuen DSGVO-Anforderungen anpassen.
- Unternehmen müssen Protokoll über zum Schutz vor Datenschutzverletzungen ergriffene Maßnahmen führen.

Die Maßnahmenpläne

- Führen Sie detaillierte Unterlagen zum Datenfluss innerhalb des Unternehmens: wie Daten erhoben werden, wie auf sie zugegriffen wird, wie sie geteilt werden und wer der Besitzer ist.
- Stellen Sie Sicherheitsrichtlinien auf, um Datenschutzverletzungen zu vermeiden. Dies umfasst:
  - Überwachung des Unternehmensnetzwerks auf Anomalien.
  - Nachverfolgung des Benutzerverhaltens, insbesondere bei Benutzern mit der Berechtigung, die persönlichen Daten zu verarbeiten.
  - Prüfung der Datei und des Ordners, in der bzw. dem persönliche Daten gespeichert werden. Lassen Sie sich benachrichtigen, wann immer unangemessene oder unbefugte Zugriffsversuche auf die persönlichen Daten erfolgen.
  - Gewährleisten Sie ordnungsgemäße organisatorische und technische Maßnahmen, um das Unternehmensnetzwerk vor Angriffen und Bedrohungen zu schützen.

Benachrichtigungen über Datenschutzverletzungen

Die DSGVO definiert eine Verletzung des Schutzes persönlicher Daten als „Sicherheitsverletzung, die zur Zerstörung, dem Verlust, der Änderung, der unbefugten Offenlegung oder dem Zugriff auf persönliche Daten führt“.

Das bedeutet, dass eine Datenschutzverletzung mehr ist als nur der Verlust von Daten. Die Vorschrift zwingt Unternehmen ebenfalls dazu, Datenschutzverletzungen „ohne unangemessene Verzögerungen und soweit möglich“ innerhalb von 72 Stunden zu melden.

Anforderungen:

- Unternehmen sollten eine angemessene interne Meldeprozedur für Datenschutzverletzungen besitzen.
- Unternehmen müssen Lieferkettenüberprüfungen und regelmäßige Audits durchführen, um sicherzustellen, dass sie die neuen Sicherheitsanforderungen erfüllen.
- Unternehmen sollten ein angemessenes technologisches Sicherheitssystem implementieren, das die sofortige Erkennung von Datenschutzverletzungen vereinfacht. Das System sollte ebenfalls umfassende Informationen bieten, um die Reaktion auf oder die Eindämmung der Datenschutzverletzung so früh wie möglich zu beschleunigen.

Die Maßnahmenpläne

- Identifizieren Sie die Kompromittierungsidentifikatoren (Indicators of Compromise, IoC), welche Sicherheitsverletzungen im Netzwerk auslösen und verfassen Sie Sicherheitsrichtlinien, um sie zu schützen.
- Implementieren Sie Sicherheitssysteme wie Firewalls und IDS/IPS, mit denen Sicherheitsangriffe verhindert werden können.
- Erwägen Sie die Implementierung von Sicherheitslösungen bei Unternehmen, die Sicherheitsverletzungen sofort erkennen, melden und darüber berichten können. Die Lösungen sollten ebenfalls in der Lage sein, bei Vorfällen oder versuchten Sicherheitsverletzungen in Echtzeit Benachrichtigungen zu versenden.
- Setzen Sie Sicherheitsrichtlinien um, die die Datenintegrität gewährleisten, indem sie folgende unbefugte Aktivitäten bei persönlichen Daten erkennen:
    - Zugriff oder Zugriffsversuche
    - Löschung
    - Teilen
    - Kopieren oder der Versuch des Kopierens
- Überwachen Sie das Verhalten berechtigter Benutzer (d. h. Benutzer, die Zugriff auf persönliche Daten haben), um im Falle eines Identitätsdiebstahls ungewöhnliche Aktivitäten zu erkennen, und melden sie diese sofort.

Die Rechte von Datensubjekten

Jegliche Handlungen, die Sie mit Daten durchführen können, gelten als Datenverarbeitung. Die DSGVO definiert jedoch enge Grenzen dafür, was Unternehmen mit erhobenen persönlichen Informationen tun und nicht tun dürfen.

Recht auf Information: Dies beginnt ab dem Zeitpunkt der Datenerhebung. Unternehmen müssen die Datensubjekte mit einer Datenschutzerklärung darüber informieren, dass die gesammelten Informationen transparent und nach Treu und Glauben verarbeitet werden. Ebenfalls müssen Unternehmen eine eindeutige und gültige Einwilligung von den Datensubjekten zur Verarbeitung der persönlichen Informationen erlangen, und zwar über ein einfach formuliertes Einwilligungsdokument.

Recht auf Zugriff: Datensubjekte oder Personen müssen jederzeit in der Lage sein, auf ihre persönlichen Informationen zuzugreifen. Mit dieser Anforderung stellt die DSGVO sicher, dass die Personen überprüfen können, ob ihre Informationen nach Treu und Glauben verarbeitet werden.

Recht auf Nachbesserung: Wenn Personen der Auffassung sind, dass ihre persönlichen Daten unvollständig oder nicht korrekt sind, haben sie das Recht, das Unternehmen um Nachbesserung zu bitten. Wenn eine Nachbesserungsanforderung eingereicht wurde, liegt es in der Verantwortung des Datenverantwortlichen, den betroffenen Personen umgehend Informationen zu ergriffenen Maßnahmen zur Verfügung zu stellen.

Recht auf eingeschränkte Datenverarbeitung: Wenn die Datenverarbeitung eingeschränkt ist, kann der Verantwortliche die Daten nur speichern, darf sie aber in keiner Weise verarbeiten. Personen können die Datenverarbeitung einschränken lassen, wenn:

- die Daten für nicht korrekt oder unvollständig befunden wurden.
- die Daten unrechtmäßig verarbeitet werden.
- der Verantwortliche keinen Grund mehr hat (gemäß der Datenschutzprinzipien), die persönlichen Daten zu verarbeiten.

Recht auf Datenübertragbarkeit: Personen müssen ihre Daten jederzeit und ohne Hindernisse abrufen und zur Verarbeitung einem anderen Verantwortlichen übertragen können. Dieses Recht gestattet es Personen, persönliche Daten auf sichere Art und Weise von einer Umgebung in eine andere zu verschieben, zu kopieren oder zu übertragen.

Recht auf Vergessenwerden: Die DSGVO gewährt Personen das volle Recht, die Löschung oder Entfernung ihrer persönlichen Daten zu fordern. Die Forderung nach Datenlöschung kann unter folgenden Umständen eingereicht werden:

- Wenn die Speicherung persönlicher Daten im Sinne des Zwecks, für den sie ursprünglich erhoben oder verarbeitet wurden, nicht länger notwendig ist.
- Wenn die Person die Einwilligung zur Datenverarbeitung zurückzieht.
- Wenn das Datensubjekt eine Anforderung einreicht, die Datenverarbeitung zu stoppen, etwa bei einer unrechtmäßigen Datenverarbeitung oder nach einer Datenschutzverletzung.
- Wenn die Daten gelöscht werden müssen, um gesetzliche Vorgaben zu erfüllen.

Die Maßnahmenpläne

- Entwerfen Sie ein ordnungsgemäßes Einwilligungsformular oder eine Datenschutzerklärung, um eine eindeutige und explizite Einwilligung von Personen zur Verarbeitung persönlicher Daten zu erhalten.
- Dokumentieren Sie Datenverarbeitungstechniken und -flüsse, damit Sie diese Personen auf Anfrage im Rahmen des Zugriffsrechts zur Verfügung stellen können.
- Ergreifen Sie technische Maßnahmen, um persönliche Daten nach Erfüllung ihres Zwecks automatisch zu löschen.
- Stellen Sie während der Datenspeicherung sicher, dass die Integrität der Daten durch Verschlüsselung gewahrt wird.
- Dokumentieren Sie die Verschlüsselungsinformationen und stellen Sie sie den Datensubjekten bei Bedarf zur Verfügung.

Strafen bei Compliance-Verstößen

Wenn Unternehmen gegen die DSGVO-Anforderungen verstoßen, können die zuständigen Behörden eine Strafe in Höhe von bis zu ***10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes des vorherigen Geschäftsjahres*** verhängen, abhängig davon, welcher Betrag höher ist. Datenverantwortliche und Datenverarbeiter riskieren diese enorme Geldstrafe, wenn die folgenden Anforderungen verletzt werden:

- Die Hauptdatenschutzprinzipien
- Datenverarbeitungsbedingungen für nicht persönliche Daten
- Einwilligungsbedingungen
- Bedingungen für die Verarbeitung empfindlicher persönlicher Daten
- Rechte von Datensubjekten

Der die Strafe verhängende Datenschutzkommissar berücksichtigt bei der Festlegung der Höhe der Strafe die Art und Schwere des Verstoßes, die ergriffenen Gegenmaßnahmen, die umgesetzten technischen und organisatorischen Maßnahmen und andere Faktoren.

Erfüllung von DSGVO-Compliance-Anforderungen mit den IT-Sicherheitslösungen von ManageEngine

Das Portfolio an IT-Sicherheitslösungen von ManageEngine umfasst eine breite Palette an Werkzeugen, mit denen Unternehmen die DSGVO-Vorgaben erfüllen können. Dazu zählen:

- **Log360**, ein umfassendes SIEM-Tool, mit dem Unternehmen Datendiebstähle erkennen, die Sicherheit gespeicherter persönlicher Daten gewährleisten und Zugriffe auf persönliche Daten nachverfolgen können. Damit kann der Rechenschaftspflicht nachgekommen werden.
- **File Audit Plus**, ein Echtzeit-Tool für Datei-Auditing und -Überwachung, das kritische Änderungen an Dateien und Ordnern mit persönlichen Daten nachverfolgt.

Wie unsere Lösungen dazu beitragen, die DSGVO-Vorgaben zu erfüllen

- **Die technischen und organisatorischen Maßnahmen, um sich vor Sicherheitsverletzungen zu schützen:** Die Bereitstellung von Log360 und File Audit Plus kann der technische Schritt sein, mit denen sich Unternehmen vor Sicherheitsverletzungen schützen können. Diese Lösungen haben die Möglichkeit, die Aktivitäten aller Geräte und Benutzer im Netzwerk zu überwachen und melden Anomalien sofort den Administratoren. Der Sicherheitsexperte kann den Vorfall dann mit den umfassenden Berichten weiter analysieren. Wird der Vorfall als Sicherheitsverletzung (oder Verletzungsversuch) eingestuft, können sofortige Maßnahmen ergriffen werden.
- **Daten-Auditing:** Die Echtzeit-Dateiintegritätsüberwachung von File Audit Plus überwacht kritische Daten kontinuierlich auf Änderungen. Ebenfalls wird eine Vielzahl von Informationen dazu bereitgestellt, wer auf die Daten zugegriffen hat, wann auf sie zugegriffen wurde und von wo aus. Der detaillierte Bericht liefert Datensubjekten Informationen zum Datenzugriff und überwacht ebenfalls Datenflüsse.
- **Durchführung von Audit-Trails:** Mit der leistungsstarken Protokollsuche von Log360 wird die forensische Analyse zum Kinderspiel Eine der Anforderungen der DSGVO besteht darin, die Grundursache der Datenverletzung oder des Verletzungsversuches zu identifizieren, um eine sofortige Gegenmaßnahme zu ergreifen. Unsere Lösung kann die Grundursache einer Datenschutzverletzungen identifizieren, indem innerhalb weniger Minuten ganze Terabytes an Protokolldaten durchsucht werden. Die Lösung bietet ebenfalls die Option, die Suchergebnisse als forensischen Bericht zu exportieren, damit dieser an die DPOs weitergeleitet werden kann. Ebenfalls kann die Suchanfrage in ein Benachrichtigungsprofil umgewandelt werden, um zukünftige Sicherheitsangriffe der gleichen Art zu bekämpfen.

EventLog Analyzer und seine Rolle bei der Erfüllung der DSGVO-Vorgaben

- Die technischen und organisatorischen Maßnahmen, um sich vor Sicherheitsverletzungen zu schützen: Die Implementierung von EventLog Analyer kann der technische Schritt sein, mit denen sich Unternehmen vor Sicherheitsverletzungen schützen können. Diese Lösung hat die Möglichkeit, die Aktivitäten aller Geräte und Benutzer im Netzwerk zu überwachen und meldet Anomalien sofort den Administratoren. Der Sicherheitsexperte kann den Vorfall dann mit den umfassenden Berichten der Lösung weiter analysieren. Wird der Vorfall als Sicherheitsverletzung (oder Verletzungsversuch) eingestuft, können sofortige Maßnahmen ergriffen werden.
- Daten-Auditing: Die Dateiintegritätsüberwachung von EventLog Analyer überwacht kritische Daten kontinuierlich auf Änderungen. Ebenfalls wird eine Vielzahl von Informationen dazu bereitgestellt, wer auf die Daten zugegriffen hat, wann auf sie zugegriffen wurde und von wo aus. Der detaillierte Bericht liefert Datensubjekten Informationen zum Datenzugriff und überwacht ebenfalls Datenflüsse.
- Durchführung von Audit-Trails: Mit der leistungsstarken Protokollsuche von EventLog Analyzer wird die forensische Analyse zum Kinderspiel Eine der Anforderungen der DSGVO besteht darin, die Grundursache der Datenverletzung oder des Verletzungsversuches zu identifizieren, um eine sofortige Gegenmaßnahme zu ergreifen. Unsere Lösung kann die Grundursache einer Datenschutzverletzungen identifizieren, indem innerhalb weniger Minuten ganze Terabytes an Protokolldaten durchsucht werden. Die Lösung bietet ebenfalls die Option, die Suchergebnisse als forensischen Bericht zu exportieren, damit dieser an die DPOs weitergeleitet werden kann. Ebenfalls kann die Suchanfrage in ein Benachrichtigungsprofil umgewandelt werden, um zukünftige Sicherheitsangriffe der gleichen Art zu bekämpfen.
- Erfüllung der Anforderung zu Datenschutzfolgenabschätzungen: die umfassenden Berichte und Benachrichtigungsprofile von EventLog Analyzer erkennen jegliche Netzwerkanomalien und Sicherheitsverletzungsversuche sofort. So kann die Datenschutzverletzung früh gestoppt werden, während die Datenschäden und Kosten eingegrenzt werden. Damit wird diese Anforderung der DSGVO erfüllt.
- Anforderung zur Meldung von Datenschutzverletzungen: EventLog Analyzer versendet in Echtzeit E-Mail- oder SMS-Benachrichtigungen über Datenschutzverletzungen an Administratoren. Damit können Datenschutzverletzungen ohne Verzögerung bei den zuständigen Stellen gemeldet werden. Diese Lösung enthält über 600 vordefinierte Benachrichtigungsprofile, die auf verschiedenen IoCs basieren. Dabei können die Angriffe sofort und mühelos erkannt werden. Darüber hinaus bietet die Lösung auch eine Option, benutzerdefinierte Benachrichtigungsprofile zu erstellen, um interne Sicherheitsanforderungen zu erfüllen.

ManageEngine

Über ManageEngine

ManageEngine bietet Echtzeit-IT-Managementwerkzeuge, mit deren Unterstützung IT-Teams den geschäftlichen Bedarf an Echtzeit-Services und -Leistungen problemlos abdecken können. Weltweit vertrauen mehr als 60.000 etablierte und aufstrebende Unternehmen – mehr als 60 % davon Teil der Fortune 500 – auf ManageEngine-Produkte, damit auf optimale Leistung ihrer unverzichtbaren IT-Infrastruktur einschließlich Netzwerken, Servern, Anwendungen, Desktops und mehr. ManageEngine ist eine Abteilung von Zoho Corp., das weltweit Niederlassungen unterhält – unter anderem in den USA, im Vereinigten Königreich, in Indien, Singapur, Japan und China.

Über den Autor

Subhalakshmi Ganapathy arbeitet aktuell als Senior Product Marketing Analyst für IT-Sicherheitslösungen bei ManageEngine. Sie verfügt über umfassendes Wissen zu Informationssicherheit und Compliance-Management. Sie bietet strategische Beratung für Unternehmen zu Sicherheitsinformations- und Ereignismanagement (SIEM), Netzwerksicherheit und Datenschutz.

Kontakt

MicroNova ist seit mehr als zehn Jahren exklusiver Vertriebspartner für die ManageEngine-Produkte in Deutschland. Das Unternehmen unterstützt seine Kunden nicht nur bei der Auswahl, Installation und Inbetriebnahme der für sie optimal geeigneten Software, sondern steht auch als deutschsprachiger Ansprechpartner für Fragen und Probleme zur Verfügung – vor Ort oder „remote“ über die Service-Mitarbeiter in der Firmenzentrale bei München.


sales-manageengine@micronova.de | support-manageengine@micronova.de


+49 81 39 / 93 00-456


Besuchen Sie www.manageengine.de/eventloganalyzer für detaillierte Informationen zur Lösung und zu allen Merkmalen.