splunk>

WHITEPAPER

WIE MASCHINENDATEN DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG (EU-DSGVO) UNTERSTÜTZEN

Übersicht: Die Datenschutz-Grundverordnung EU-DSGVO

Im Jahr 2012 empfahl die EU-Kommission eine umfassende Reform der Datenschutzrichtlinie 95/46/EG mit einer Reihe von Datenschutzgrundsätzen, die von allen Mitgliedsstaaten in ihre lokalen Gesetze übernommen wurden. Dies führte zu einem uneinheitlichen Flickenteppich aus Datenschutzvorschriften innerhalb der EU. Dieser uneinheitliche Ansatz machte Compliance für globale Unternehmen aufwändig und schwierig.

Im April 2016 verabschiedete das Europäische Parlament die neue Datenschutz-Grundverordnung EU-DSGVO, die die uneinheitliche Vorschriftenmischung durch ein einziges, harmonisiertes Gesetz ersetzt, das für alle EU-Mitgliedsstaaten bindend ist. Die EU-DSGVO bietet Unternehmen mehr Vorhersehbarkeit und Effizienz und stärkt die Datenschutzrechte von EU-Bürgern im neuen digitalen Zeitalter. Die EU-DSGVO tritt im Mai 2018 in Kraft. Die wichtigsten Anforderungen sind:

- Mehr Rechte für Datensubjekte, etwa das Recht „vergessen zu werden“, und Datenübertragbarkeit
- Auf Sicherheit ausgerichtete Softwareentwicklung (Datenschutz standardmäßig vorgesehen)
- Pseudonymisierung oder Verschlüsselung persönlicher Daten (Datenschutz standardmäßig vorgesehen)
- Sichere Datenverarbeitung
- Meldung von Verstößen gegen die Sicherheit persönlicher Daten innerhalb von 72 Stunden
- Geldstrafen in Höhe von bis zu 20 Millionen Euro oder vier Prozent des Jahresumsatzes, je nachdem, welcher Wert höher ist

Die EU-DSGVO gilt zudem nicht nur für Unternehmen innerhalb der EU, ***sondern auch für Unternehmen in aller Welt, die ihre Waren und Dienstleistungen EU-Bürgern anbieten.***

So unterstützen Maschinendaten die Grundverordnung

Maschinendaten bieten nützliche Aufzeichnungen zu den Aktivitäten im Zusammenhang mit Kunden, Benutzern, verarbeiteten Transaktionen, Anwendungen, Servern, Netzwerken und Mobilgeräten. Aus Maschinendaten gewonnene Erkenntnisse helfen bei vielen Problemstellungen im gesamten Unternehmen und können auch mit Daten aus anderen Quellen kombiniert werden. Wir haben drei Anwendungsfälle zusammen gestellt, die Sie bei der Implementierung der Datenschutz-Grundverordnung unterstützen und unabhängig von Branche und Systemarchitektur (lokal, cloud-basiert oder hybrid) zutreffen.

1. Sicherheitsmanagement und Melden von Verstößen

Artikel 32 – Sicherheit der Verarbeitung

Szenario: Ein Mitarbeiter Ihrer Personalabteilung erhält eine gezielte Phishing-E-Mail, in der er aufgefordert wird, sein Systempasswort zurückzusetzen. Da die Phishing-E-Mail von Ihrem Spam-Filter nicht blockiert wurde und die Textformatierung der rechtmäßiger E-Mails entsprach, klickte der Mitarbeiter auf den Link, wodurch seine Zugangsdaten den Angreifern in die Hände fielen. Die gleichen Zugangsdaten werden von dem Mitarbeiter für den Zugriff auf Ihr Personaldatensystem verwendet, und somit sind die persönlichen Daten der gesamten Belegschaft gefährdet.

Die EU-DSGVO fordert Sicherheit der Verarbeitung (Artikel 32), das heißt, Unternehmen, die persönliche Daten verarbeiten, müssen „geeignete technische und organisatorische Maßnahmen“ implementieren, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Dies umfasst dem Stand der Technik entsprechende Maßnahmen zur Verhinderung des unbefugten Zugriffs auf personenbezogene Daten.

Aus Maschinendaten gewonnene Erkenntnisse ermöglichen die frühzeitige Warnung vor Bedrohungen in Ihrer digitalen Infrastruktur. Ihre digitale Umgebung produziert riesige Mengen an Aktivitätsprotokollen, die zum Erkennen von Anomalien im Benutzerverhalten sowie zum Aufdecken von nicht autorisiertem Zugriff genutzt werden können. Maschinendaten können beispielsweise Auskunft darüber geben, ob Anmeldeaktivitäten im Zusammenhang mit einem Mitarbeiter vorliegen, der wegen Urlaubs oder Krankheit gar nicht im Büro ist, und eine Warnmeldung ausgeben. Sie können auch feststellen, wenn sich ein neues Mobilgerät bei Ihrem System oder über VPN anmeldet. So werden Sie frühzeitig vor kompromittierten Zugangsdaten gewarnt und können einen Datenabfluss verhindern. Maschinendatenanalysen liefern solche Ergebnisse schnell und in Echtzeit.

Artikel 33 und 34 – Meldung und Benachrichtigung

Die EU-DSGVO fordert die Benachrichtigung bei Verletzungen des Schutzes personenbezogener Daten. Das heißt, das Unternehmen muss eine Verletzung des Schutzes personenbezogener Daten, die ein Risiko für die Rechte und Freiheiten von EU-Bürgern darstellt, innerhalb von 72 Stunden nach deren Bekanntwerden an die zuständige Aufsichtsbehörde melden (Artikel 33) sowie unverzüglich die betroffenen Personen benachrichtigen (Artikel 34). Die Meldung muss u. a. Informationen über *die Art der Verletzung des Schutzes personenbezogener Daten mit Angabe der Zahl der betroffenen Datensubjekte* sowie die ergriffenen Abhilfemaßnahmen enthalten.

„Angesichts des engen Zeitrahmens für das Melden einer Sicherheitsverletzung ist es besonders wichtig, robuste Prozesse für die Erkennung, Untersuchung und interne Meldung von Sicherheitsverletzungen zu implementieren."

ICO (Information Commissioner's Office) über die Meldepflicht der EU-DSGVO

Aus Maschinendaten gewonnene Erkenntnisse ermöglichen Unternehmen, Sicherheitsverletzungen schnell aufzuspüren und zu untersuchen sowie ihren Umfang abzuschätzen. Mit detaillierten Analysen lässt sich ermitteln, wie und wann der Angreifer in die Umgebung eindrang, auf welche Systeme wann zugegriffen wurde, wie viele Personen oder Datensätze betroffen sind und, welche Abwehrmaßnahmen ergriffen werden müssen. All dies unterstützt Sie dabei, die Anforderungen der Meldepflicht zu erfüllen.

2. Datenschutzüberprüfungen

Artikel 58 – Befugnisse

Szenario: Es gab eine Sicherheitsverletzung aufgrund einer unbekannten Schwachstelle: Sie haben den Umfang des Angriffs abgeschätzt, festgestellt, dass personenbezogene Daten offengelegt wurden, die betroffenen Personen identifiziert, die Sicherheitsverletzung gemeldet und Abwehrmaßnahmen ergriffen, um das Risiko einzudämmen. Jetzt fordern die betroffenen Personen Schadenersatz, und die Aufsichtsbehörde fordert Sie auf, eine Datenschutzüberprüfung durchzuführen, um festzustellen, ob Ihre Sicherheitsmaßnahmen „dem Stand der Technik entsprechende" Technologien zum Schutz der Verarbeitungsprozesse umfassen.

Die EU-DSGVO gibt den einzelnen Aufsichtsbehörden die Befugnis, Untersuchungen in Form von Datenschutzüberprüfungen durchzuführen, Warnhinweise zu geben, Verwarnungen auszusprechen und sogar Datenverarbeitungsverbote zu verhängen (Artikel 58). Außerdem sind die Behörden ermächtigt, Geldbußen in Höhe von bis zu 20 Millionen Euro oder vier Prozent des gesamten weltweiten Jahresumsatzes eines Unternehmens zu verhängen, je nachdem, welcher Wert höher ist. Darüber hinaus hat laut Artikel 82 jede Person, der ein materieller oder immaterieller Schaden entstanden ist, Anspruch auf Schadenersatz. Geldbußen lassen sich nur abwenden, wenn der Verantwortliche nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist. Dazu müssen Unternehmen ihre Aktionen dokumentieren und die Einhaltung der Vorschriften gegenüber der Aufsichtsbehörde nachweisen.


```
{ [-]
   ClientIP: 101.235.6.6
   CreationTime: 2017-04-11T03:32:43
   EventSource: SharePoint
   Id: 2af64672-f9ca-4c25-0274-08d40c2fb043
   ItemType: File
   ListItemUniqueId: 43b04c3c-8a3f-400e-8c9c-d79addbfc112
   ObjectId: https://broncos-my.sharepoint.com/personal/anthony_milford_broncos_com_au/Documents/Copy of Asset player HR
Actions  Recruitment Report (AE 1).XLS
   Operation: FileUploaded
   OrganizationId: a74a1efc-372d-476c-802c-9cbbe5a5c71e
   RecordType: 6
   Site: d983b062-461e-4ef5-b237-2fafe2071f0f
   SiteUrl: https://broncos-my.sharepoint.com/personal/anthony_milford_broncos_com_au/
   SourceFileExtension: XLS
   SourceFileName: Copy of Asset player HR Actions  Recruitment Report (AE 1).XLS
   SourceRelativeUrl: Documents
   UserAgent: Microsoft SkyDriveSync 17.3.6517.0809 ship; Windows NT 10.0 (10586)
   UserId: anthony.milford@broncos.com.au
   UserKey: i:0h.f|membership|10033fff8ae39bf3@live.com
   UserType: 0
   Version: 1
   WebId: c6820655-bf56-425d-b22d-41fd55da3045
   Workload: OneDrive
}
```


Beispiel für Maschinendaten über den Zugriff auf eine Datei mit personenbezogenen Daten

Maschinendaten liefern die historischen Informationen, die Unternehmen benötigen, um gegenüber den Kontroll- und Aufsichtsbehörden nachzuweisen, dass angemessene Sicherheitsvorkehrungen eingerichtet und proaktiv zur Risikominimierung eingesetzt wurden. Egal, ob es sich um technische Konfigurationen und ihre Änderungen oder den Verlauf von Passwortrücksetzungen bzw. -aktualisierungen handelt, Maschinendaten können genutzt werden, um alle diese Aktionen und viele andere wichtige Sicherheitsfaktoren zu dokumentieren.

3. Auskunftsrecht über die Verarbeitung personenbezogener Daten

Artikel 15, 17, 18 und 28 (Rechte von Datensubjekten)

Beispielszenario: Ihr Unternehmen ist Dienstleister für Lohn- und Gehaltsabrechnung für kleine Unternehmen in ganz Europa. Infolgedessen verarbeiten Sie jeden Monat große Mengen personenbezogener Daten und werden ab und zu von Kunden gebeten, Berichte über die Datenverarbeitung bereitzustellen. Bei einem Ihrer früheren Kunden kam es vor kurzem zu einer Sicherheitsverletzung. Dieser Kunde wendet sich nun im Zuge einer Datenschutzüberprüfung durch die Aufsichtsbehörde an Sie als Auftragsverarbeiter. Sie werden gebeten, in einem Bericht zu dokumentieren, wer in Ihrem Unternehmen in den letzten 12 Monaten auf die personenbezogenen Daten des Kunden zugegriffen hat. Außerdem sollen Sie nachweisen, dass Sie die personenbezogenen Daten des Kunden aus Ihrem System (und allen Sicherungskopien) entfernt haben, nachdem der Vertrag beendet wurde.

Die EU-DSGVO gibt EU-Bürgern das Recht zu erfahren, welche personenbezogenen Daten über sie verarbeitet werden, für wen diese freigegeben werden und, wo die Datenverarbeitung erfolgt (Artikel 15). Datensubjekte können zudem verlangen, dass ihre personenbezogenen Daten berichtigt (Artikel 16) oder gelöscht werden (Artikel 17). Die Verantwortlichen müssen sicherstellen, dass die personenbezogenen Daten nur von autorisierten Personen verarbeitet werden. Wenn die Verarbeitung abgeschlossen und der Vertrag beendet ist, kann ein Unternehmen vom Auftragsverarbeiter verlangen, dass alle personenbezogenen Daten gelöscht oder zurückgegeben werden. Dies gilt auch für eventuell existierende Sicherungskopien.

Maschinendaten geben Unternehmen End-to-End-Transparenz bei ihren Verarbeitungsaktivitäten – dies sind kritische Informationen für die EU-Datenschutzgrundverordnung. Mithilfe von Maschinendaten können Sie belegen, auf welche personenbezogenen Daten zugegriffen wurde und von wem, wie die Daten genutzt wurden, und nachweisen, wann sie gelöscht wurden.

Tausende von Unternehmen setzen auf die Splunk-Plattform, um die Sicherheit zu erhöhen, die Effizienz zu steigern, datenbasierte Entscheidungen zu treffen sowie taktische und strategische Vorteile zu erzielen. Jede Umgebung verfügt jedoch über ihre eigene, ganz spezifische Art von Maschinendaten. Möchten Sie mehr über Ihre Maschinendaten erfahren und einen Workshop zur EU-DSGVO durchführen? **Fragen Sie einfach uns.**

splunk> SplunkCE@splunk.com www.splunk.com

WP-Splunk-How-Machine-Data-Supports-GDPR-Compliance-A4-101