Datenschutzerklärung zur Verarbeitung personenbezogener Daten im Rahmen von Splunk

Der Schutz Ihrer Privatsphäre ist für das Europäische Patentamt (EPA) von höchster Bedeutung. Wir sind bei der Erfüllung unserer Aufgaben und der Erbringung unserer Dienstleistungen dem Schutz Ihrer personenbezogenen Daten sowie der Wahrung Ihrer Rechte als betroffener Person verpflichtet. Alle Daten persönlicher Art, die Sie direkt oder indirekt identifizieren, werden rechtmäßig, fair und mit der gebotenen Sorgfalt verarbeitet.

Die nachstehend beschriebenen Verarbeitungen erfolgen nach den Datenschutzvorschriften des EPA (DSV). Die Informationen in dieser Erklärung werden Ihnen gemäß den Artikeln 16 und 17 DSV bereitgestellt.

Splunk ist das zentrale Protokollarchiv des EPA für das Vorfallmanagement, das durch die Identifizierung und Analyse von Sicherheitsproblemen zum Schutz von EPA-Systemen beiträgt.

1. Wie erfolgt die Verarbeitung und wozu dient sie?

Die Verarbeitung von Daten mit Splunk umfasst:

- das Empfangen technischer Daten, die von anderen BIT-Systemen und -Diensten generiert wurden und bereits verfügbar sind
- automatische Abfragen zur Generierung von Warnungen bei relevanten Sicherheitsereignissen
- automatisierte Abfragen zur Generierung von Dashboards und Übersichten mit sicherheitsrelevanten Informationen
- manuelle Abfragen für eine eingehendere Analyse von Sicherheitsereignissen, die Anpassung von Dashboards sowie Warnmeldungen

Splunk empfängt technische Daten, die in verschiedenen EPA-Systemen und -Diensten generiert wurden (und verfügbar sind), insbesondere

- auf EPA-verwalteten Workstations, die EPA-Nutzern zugewiesen sind
- auf EPA-verwalteten Servern
- auf EPA-verwalteten Netzwerkgeräten (z. B. Routern, Switches, Firewalls und Proxy-Servern)
- bei externen Cloud-Anbietern im Rahmen eines Vertragsverhältnisses mit dem EPA (z. B. Microsoft, Google, Amazon und SAP)

Personenbezogene Daten werden verarbeitet, um die Personen zu identifizieren, die die protokollierten Aktivitäten durchgeführt haben, damit eventuelle Fehler oder festgestellte Sicherheitsprobleme behoben werden können. Dies ist aus folgenden Gründen wichtig:

- Protokolldateien werden verwendet, um Ereignisse in einem Informationssystem nachzuverfolgen und die Fehlerbehebung und Reparatur zu unterstützen. Sie sind Teil des Systems und unerlässlich, um Sicherheit und effiziente Unterstützung zu gewährleisten, wenn Informationssysteme nicht ordnungsgemäß funktionieren.
- Protokolldateien von EPA-Systemen werden verarbeitet, um Sicherheitsvorfälle und Malware-Infektionen auf mit dem EPA-Netzwerk verbunden Geräten zu untersuchen und zu beheben und/oder um Datenlecks zu verhindern.
- Darüber hinaus können Protokolldateien zu statistischen Zwecken oder zur Lösung von Problemen mit dem Nutzerzugriff auf EPA-Telekommunikationssysteme verarbeitet werden.

Die Verarbeitung ist nicht zur Verwendung für eine automatisierte Entscheidungsfindung (einschließlich Profiling) gedacht.

Ihre personenbezogenen Daten werden nicht an Empfänger außerhalb des EPA übermittelt.

2. Welche personenbezogenen Daten verarbeiten wir?

Über Splunk sammelt der delegierte Verantwortliche, BIT HD 4.6, personenbezogene Daten, wenn solche Daten in die vom Ursprungssystem generierten Protokolle aufgenommen werden. Besondere Kategorien personenbezogener Daten werden über Splunk nicht wissentlich oder absichtlich erhoben.

Verarbeitete personenbezogene Daten können sich auf EPA-Bedienstete, Auftragnehmer des EPA oder Externe beziehen.

Verarbeitete personenbezogene Daten, wenn die betroffene Person EPA-Bediensteter oder Auftragnehmer des EPA ist:

- persönliche Identifikationsdaten: vollständiger Name (Vorname/Nachname) und Geschlecht
- Kontaktinformationen: geschäftliche E-Mail-Adresse, Telefonnummern
- Nutzerkontodaten: Nutzer-ID, Kontonummer
- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsmetadaten
- Systemprotokolle: laufende Prozesse, Registry-Daten, Dateimetadaten (Dateiname, Größe, Hash), Portnummern, transaktionsbezogene Details, Überwachungsprotokolle, system-, anwendungs- und sicherheitsbezogene Serverprotokolle, Webserver-Protokolle, Firewall-/Router-/Switch-Protokolle
- Kennungen von physischen/digitalen Anlagen, die die betroffene Person zur Verbindung mit EPA-Systemen verwendet hat: Seriennummer, Hostname und Betriebssystemversion der Workstation, MAC-Adresse der Netzwerkschnittstelle
- Browsing-Informationen: Browsertyp, URL, Browser-Nutzer-Agent, Datum und Uhrzeit, IP-Adresse, Kategorie, Websiteverlauf, Netzwerkinteraktionsverlauf
- Anrufdaten: Anrufernummer, angerufene Nummer, Datum und Uhrzeit, Dauer, Interaktionsverlauf
- Telefonie-Interaktionsdaten: Metadaten der Telefoniesitzung
- Beschäftigungsdaten: Indikator aktiv/inaktiv, Enddaten, Abteilungsbezeichnung und/oder -nummer, Zimmernummer, Bürostandort, Stellenbezeichnung, Jobgruppe (nur für Bedienstete), Startdatum, Vorgesetzter, bevorzugte Sprache (für Kommunikation), Vertragstyp, Personalnummer
- Ticket-bezogene Daten
- Standortinformationen

Verarbeitete personenbezogene Daten, wenn die betroffene Person eine externe Person ist:

- Netzwerk-/Anwendungs-Interaktionsdaten: Sitzungsmetadaten
- Systemprotokolle: Firewall-/Router-/Switch-Protokolle, Webserver-Protokolle, system-, anwendungs- und sicherheitsbezogene Serverprotokolle
- Kennungen von physischen/digitalen Anlagen, die die betroffene Person zur Verbindung mit EPA-Systemen verwendet hat: Hostname und Betriebssystemversion der Workstation, MAC-Adresse der Netzwerkschnittstelle
- Browsing-Informationen: Browsertyp, URL, Browser-Nutzer-Agent, Datum und Uhrzeit, IP-Adresse, Kategorie, Websiteverlauf, Netzwerkinteraktionsverlauf
- Anrufdaten: Anrufernummer, angerufene Nummer, Datum und Uhrzeit, Dauer, Interaktionsverlauf
- Telefonie-Interaktionsdaten: Metadaten der Telefoniesitzung
- Ticket-bezogene Daten

3. Wer ist für die Verarbeitung der Daten verantwortlich?

Personenbezogene Daten im Rahmen von Splunk werden unter der Verantwortung der Hauptdirektion 4.6 CIO/BIT verarbeitet, die als delegierter Datenverantwortlicher des EPA handelt.

4. Wer hat Zugriff auf Ihre personenbezogenen Daten und für wen werden sie offengelegt?

Personenbezogene Daten im Rahmen von Splunk werden nur von Empfängern in den BIT-Abteilungen 4.6.2.3 Informationssicherheit und 4.6.3.8 Netzwerk- und Rechenzentrumverwaltung für notwendige Verarbeitungen abgerufen.

Splunk wird ausschließlich nach dem Prinzip der Erforderlichkeit von der BIT-Abteilung 4.6.2.3 Informationssicherheit zur Unterstützung der Sicherheitsgewährleistung und von der BIT-Abteilung 4.6.3.8 Netzwerk- und Rechenzentrumverwaltung zur Unterstützung der Netzverwaltung verwendet.

Externe Auftragnehmer können gelegentlich im Rahmen der Wartung von Splunk personenbezogene Daten aus Splunk verarbeiten (und darauf zugreifen).

5. Wie schützen wir Ihre personenbezogenen Daten?

Wir ergreifen geeignete technische und organisatorische Maßnahmen, um Ihre personenbezogenen Daten vor unbeabsichtigter oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung bzw. unbefugtem Zugang zu schützen.

Alle personenbezogenen Daten im Rahmen der existierenden Verarbeitung werden gemäß dem Informationssicherheitsrahmen des EPA in einer sicheren, internen IT-Anwendung gespeichert.

Physische Sicherheit: In den EPA-Gebäuden finden physische Zugangskontrollen statt; in den EPA-Rechenzentren in Luxemburg und München sind zusätzliche Zugangskontrollen in Betrieb.

Logische Sicherheit: Härtung wird auf Systeme, Geräte und Netzwerke angewendet.

Zugriffskontrolle: Die Systeme und das Netzwerk unterliegen einer rollenbasierten Zugriffskontrolle nach den Grundsätzen der Bedarfsorientiertheit und der minimalen Berechtigung; Administrator- und Nutzerrollen sind getrennt; umfassende Administratorrechte werden auf das Minimum beschränkt.

Der Zugriff auf Splunk ist rollenbasiert. Active-Directory-Gruppen bestimmen, welche Rollen Nutzern zugewiesen sind; die Rollen schränken ein, auf welche Art von Informationen in Splunk zugegriffen werden kann. Angemessene Zugriffsberechtigungen werden individuell nur den oben genannten Empfängern gewährt.

Nutzerauthentifizierung: Alle Workstations und Server benötigen eine Anmeldung, mobile Geräte benötigen eine Anmeldung für den EPA-internen Bereich, privilegierte Konten benötigen eine zusätzliche und strengere Authentifizierung. Alle Abfragen über Splunk werden von authentifizierten Nutzern ausgeführt. Die Authentifizierung basiert auf Active-Directory-Systemen des EPA und stellt so sicher, dass eine durchgängige Kontoverwaltung umgesetzt wird (z. B. Deaktivierung der Konten von Bediensteten, die das Amt verlassen).

Protokollierung: Splunk dokumentiert vollständig alle Nutzerabfragen und sonstigen Aktivitäten. Diese Informationen haben wie alle anderen Informationen in Splunk den Status "append only" (=nur anfügen), d. h. sie können nach der Eintragung nicht mehr unentdeckt geändert oder entfernt werden.

6. Wie können Sie auf Ihre Daten zugreifen, sie berichtigen oder sie erhalten? Wie können Sie die Löschung Ihrer Daten verlangen oder ihre Verarbeitung beschränken bzw. ihr widersprechen? Können Ihre Rechte beschränkt werden?

Sie haben das Recht, auf Ihre personenbezogenen Daten zuzugreifen, sie zu berichtigen und sie zu erhalten, das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, sowie das Recht, Ihre Daten löschen zu lassen und die Verarbeitung Ihrer Daten zu beschränken und/oder ihr zu widersprechen (Artikel 18 bis 24 DSV).

Wenn Sie von einem dieser Rechte Gebrauch machen möchten, wenden Sie sich bitte schriftlich unter DP_BIT@epo.org an den delegierten Datenverantwortlichen. Damit wir schneller und genauer darauf antworten können, sollten Sie uns mit Ihrem Antrag stets bestimmte Vorabinformationen übermitteln. Deshalb bitten wir Sie, als externer Nutzer dieses Formular und als interner Nutzer dieses Formular auszufüllen und zusammen mit Ihrem Antrag einzureichen.

Wir werden Ihren Antrag baldmöglichst und in jedem Fall innerhalb eines Monats nach Eingang des Antrags bearbeiten. Gemäß Artikel 15 (2) DSV kann dieser Zeitraum jedoch um zwei Monate verlängert werden, wenn es aufgrund der Komplexität und der Zahl der eingegangenen Anträge erforderlich ist. Wir werden Sie in diesem Fall entsprechend informieren.

7. Auf welcher Rechtsgrundlage basiert die Verarbeitung Ihrer Daten?

Personenbezogene Daten werden gemäß Artikel 5 a) DSV verarbeitet: Die Verarbeitung ist für die Wahrnehmung einer Aufgabe in Ausübung der amtlichen Tätigkeit der Europäischen Patentorganisation oder in rechtmäßiger Ausübung dem Verantwortlichen übertragener öffentlicher Gewalt, was die für die Verwaltung und die Arbeitsweise des Amts notwendige Verarbeitung einschließt, erforderlich.

Personenbezogene Daten werden auf folgender Rechtsgrundlage verarbeitet: Rundschreiben Nr. 382 vom 29. März 2017 – Richtlinien des EPA für die Informationssicherheit, Artikel 7 "Überwachung, Kontrolle, Auditierung und weitere Verarbeitung".

8. Wie lange speichern wir Ihre Daten?

Personenbezogene Daten im Rahmen von Splunk werden nur so lange gespeichert, wie es für die Zwecke der Verarbeitung erforderlich ist.

Die in Splunk vor Ort gespeicherten Daten unterliegen der normalen Backup- und Archivierungsrichtlinie für Server vor Ort.

Splunk-Protokolldateien werden automatisch gespeichert und je nach Art der Information und System, auf das sie sich beziehen, für einen vereinbarten Zeitraum aufbewahrt. Daten von Microsoft Defender für Endpoint zu Sicherheitswarnungen und -ereignissen werden 12 Monate in Splunk aufbewahrt. Andere Daten werden bis zu 18 Monate in Splunk aufbewahrt und danach automatisch gelöscht. Die Daten werden nach dem Entfernen aus dem Splunk-System für 60 Tage in Backups aufbewahrt, danach sind sie nicht mehr verfügbar. Das heißt, die Datenaufbewahrung in Splunk überschreitet nie 20 Monate.

Im Falle einer förmlichen Beschwerde/Rechtsstreitigkeit werden alle Daten, die bei Einleitung der förmlichen Beschwerde/Rechtsstreitigkeit gespeichert waren, bis zum Abschluss des Verfahrens aufbewahrt.

9. Kontaktinformationen

Bei Fragen zur Verarbeitung der personenbezogenen Daten können EPA-Bedienstete schriftlich den delegierten Datenverantwortlichen unter DP_BIT@epo.org kontaktieren, externe betroffene Personen wenden sich bitte an DPOexternalusers@epo.org.

Die Datenschutzbeauftragte erreichen EPA-Bedienstete unter dpo@epo.org, Externe verwenden zu diesem Zweck die Adresse DPOexternalusers@epo.org.

Überprüfung und Rechtsmittel

Wenn Sie der Ansicht sind, dass die Verarbeitung Ihre Rechte als betroffene Person verletzt, sind Sie berechtigt, gemäß Artikel 49 DSV einen Antrag auf Überprüfung durch den Verantwortlichen zu stellen, und falls Sie mit dem Ergebnis der Überprüfung nicht einverstanden sind, können Sie gemäß Artikel 50 DSV Rechtsmittel einlegen.