RED HAT® ANSIBLE® Automation

redhat.

E-BOOK

EINHALTUNG DER DSGVO MITHILFE VON AUTOMATISIERUNG

INHALTSVERZEICHNIS

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com

EINLEITUNG

Im Mai 2018 begann die Europäische Union (EU) mit der Durchsetzung der größten Änderung der Datenschutzbestimmungen in den letzten 20 Jahren. Die EU-Datenschutz-Grundverordnung (DSGVO) betrifft zahlreiche Rollen in jeder EU-Entity, die personenbezogene Daten verarbeitet.

DSGVO-Datenschutzverletzungen können schwierig zu erkennen, zu beheben und zu vermeiden sein. In großen Unternehmen und in agilen DevOps-Umgebungen kann das Erreichen von Compliance ohne Automatisierung eine große Herausforderung darstellen. Außerdem haben die vorhandenen Tools zum Erfassen, Aggregieren und Schützen von Daten häufig keine nativen Funktionen zur Einhaltung der DSGVO. Darüber hinaus bieten sie unter Umständen Programmierschnittstellen (Application Program Interface, API) und andere programmatische Zugriffsmethoden, die zur Unterstützung der Compliance automatisiert werden können.

IT-Unternehmen können Datenschutzbeauftragten in vielerlei Hinsicht bei der Bewältigung der Herausforderungen in Bezug auf die Durchsetzung der DSGVO-Compliance helfen. Eine anwenderfreundliche Automatisierungsplattform mit zentralisiertem Management und einer modularen Architektur für eine Vielzahl von Use Cases können zuverlässige DSGVO-Unterstützung bieten.

Red Hat® Ansible® Automation, eine Open Source-Automatisierungsplattform für Unternehmen, kann unabhängig oder mit anderen Tools für die Unterstützung kritischer Compliance-Funktionen eingesetzt werden, wie automatisierte Datenermittlung und -zuordnung, automatisierter Schutz vertraulicher Daten, automatisierte Beseitigung nicht konformer Daten, automatisierte Bereitstellung von Kundendaten zur Erfüllung von Anliegen in Bezug auf das Auskunftsrecht, das Löschen von Kundendaten zur Erfüllung von Anliegen in Bezug auf das Recht auf Löschung oder automatisierter Export von Kundendaten zur Erfüllung von Anliegen in Bezug auf das Recht auf Datenübertragbarkeit.

WAS IST DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG (DSGVO)?

Die DSGVO ist die EU-Reform des gültigen Rechtsrahmens für Datenschutz, mit dem die ungleichartigen nationalen Datenschutzgesetze harmonisiert werden sollen. Dabei werden umfassende Verpflichtungen für Unternehmen eingeführt, die personenbezogene Daten erfassen, verwenden oder anderweitig verarbeiten.

Im Rahmen der DSGVO dürfen personenbezogene Daten nur verarbeitet werden, wenn mindestens eine der folgenden rechtmäßigen Grundlagen zutrifft: Die betroffene Person hat ihre Einwilligung zur Verarbeitung der betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben, oder sofern eine Verarbeitung erforderlich ist:

- Für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen, die auf Anfrage der betroffenen Person erfolgen.
- Zur Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt.
- Zum Schutz der lebenswichtigen Interessen der betroffenen Person oder einer anderen natürlichen Person.
- Für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
- Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Der Geltungsbereich der DSGVO geht über die territorialen Grenzen der EU hinaus und bezieht sich auch auf Organisationen, die Personen innerhalb der EU Dienstleistungen oder Waren anbieten oder das Verhalten einer Person innerhalb der EU überwachen.

Unternehmen, die gegen die DSGVO verstoßen, können mit Geldstrafen von bis zu 4 % ihres globalen Jahreseinkommens oder in Höhe von 20 Millionen Euro belegt werden, je nachdem, welcher Betrag höher ist.

WELCHE HERAUSFORDERUNGEN BESTEHEN IN BEZUG AUF DIE DSGVO?

Im Juni 2017 gab Gartner zwei strategische Annahmen bekannt:

1. Am 25. Mai 2018 erfüllen weniger als 50 % aller betroffenen Unternehmen die Anforderungen der DSGVO vollständig.
2. Vor dem Jahr 2020 werden vorgeschriebene Sanktionen in Höhe von mehreren Millionen Euro wegen Nichterfüllung der DSGVO-Anforderungen erhoben.[1]

Laut Gartner basieren diese Annahmen auf der Komplexität hinsichtlich der Erkennung, Behebung und Vermeidung von Datenschutzverletzungen – insbesondere in großen Unternehmen und in agilen DevOps-Umgebungen.

- **Schwierig zu erkennen**, weil Kundendaten immer häufiger über verschiedene Kanäle standort- und geschäftsbereichsübergreifend – sowie in On-Premise-, Cloud- und Hybrid-Infrastrukturen – erfasst und nicht immer mithilfe einer einheitlichen Datenverwaltungsstrategie aggregiert werden. Aus dieser Diversität wächst die Herausforderung, beurteilen zu können, welche Daten verfügbar sind, für welche Daten berechtigtes Interesse besteht, welche Daten sensibel sind und geschützt werden müssen, und welche Daten beseitigt werden müssen, um die DSGVO-Anforderungen erfüllen zu können.
- **Schwierig zu beheben**, weil für die Lösungen das Ausführen umfassender Kundendatenaktivitäten erforderlich ist, wie das Hinzufügen von Pseudonymen, Tokens oder Löschsicherungen. Wenn Datensysteme keine nativen Funktionen für diese Aufgaben bereitstellen, kann alternativ auf vorhandene APIs und andere programmatische Datenzugriffsmethoden zurückgegriffen werden.
- **Schwierig zu vermeiden**, weil eine kontinuierliche Compliance signifikante Änderungen dahingehend erfordert, wie Daten erfasst werden, eine Möglichkeit zur zentralen Aggregation von Daten (z. B. Data Lakes) sowie ein System zur Automatisierung von Compliance-Prüfung und -Berichten.

Außerdem hat die EU in Bezug auf Tools und betriebliche Frameworks, die für eine Compliance erforderlich sind, keine allzu engen Vorgaben gemacht. Die nahe liegendsten Lösungen zur Einhaltung der DSGVO-Bestimmungen sind Tools zur Verwaltung von Privatsphäre und Datenschutz (wie integriertes Risikomanagement), Zustimmungs- und Cookie-Managementtools sowie Tools zur Datenschutzkontrolle, einschließlich Datenlebenszyklus-Verwaltungs- und Pseudonymtools, wie Tokenisierung und Maskierung. Diese Tools müssen jedoch automatisiert werden, um die Compliance in großem Maßstab aufrechterhalten zu können.

EINHALTUNG DER DSGVO MIT RED HAT ANSIBLE AUTOMATION

Automatisierung ist eine vielseitige und leistungsstarke Funktion, mit der eine Vielzahl von IT-Aufgaben ausgeführt werden können, wie Compute-, Netzwerk- und Storage-Infrastruktur, BS-Konfiguration, Multi-Tier-Anwendungsbereitstellung sowie die Durchsetzung von Sicherheitsrichtlinien und Compliance-Regeln.

Die Wahrscheinlichkeit ist sehr hoch, dass Ihre IT-Organisation bereits eine oder mehrere Automatisierungstools für einige dieser Aufgaben oder als Bestandteil der strategischen Initiativen wie DevOps verwendet. Je flexibler und anwenderfreundlicher Ihr Automatisierungstool ist, desto einfacher ist es, dieses Tool zur Durchsetzung der DSGVO-Compliance zu verwenden.

Laut Joerg Fritsch, Research Director im Team Security and Risk Management Strategies von Gartner, „können Technikexperten das DSGVO-Programm durch den Einsatz von Technologie unterstützen, die einen Prozess wiederholbar und skalierbar macht.“[2]

Red Hat Ansible Automation ist eine IT-Automatisierungsplattform mit einer leicht zu erlernenden Sprache, leistungsstarken zentralisierten Management-Features und einer modularen Architektur, mit der Probleme bei der DSGVO-Compliance in zahlreichen Szenarios angegangen werden können.

1 „GDPR Clarity: 19 Frequently Asked Questions Answered“. Gartner. 29 Aug. 2017.

2 *Fritsch, Joerg. „A Technical Solution Landscape to Support Selected GDPR Requirements“. Gartner. Feb. 2018.*

USE CASE 1: VERTRAULICHE DATEN MIT AUTOMATISIERTER DATENERMITTLUNG UND -ZUORDNUNG ERKENNEN

In großem Maßstab wird selbst der Datenermittlungsprozess zu einer Herausforderung. Red Hat Ansible Automation kann die Ermittlung und Zuordnung elektronisch gespeicherter Informationen vereinfachen, beispielsweise mit E-Discovery-Produkten innerhalb einer kompletten IT-Infrastruktur.

Red Hat Ansible Engine arbeitet ohne Agent und stellt über SSH (Secure Shell) Verbindungen zu Zielsystemen her. IT-Teams können Automatisierungs-Workflows (oder Ansible Playbooks) schreiben, die eine einfache Sprache verwenden, um zu beschreiben oder anzuordnen, wie der E-Discovery-Agent in Zielsystemen bereitgestellt und ausgeführt wird.

Im folgenden Beispiel wird mit einem Ansible Playbook sichergestellt, dass der Agent einer E-Discovery-Lösung ordnungsgemäß installiert und gestartet wird. Falls der Agent nicht erwartungsgemäß ausgeführt wird, sendet das Playbook eine Warnmeldung:

```
- name: Ensure operating ediscovery agent
  hosts: all
  become: yes

  tasks:
    - name: Ensure latest ediscovery configuration
      template:
        src: templates/ediscovery-agent.j2
        dest: /etc/ediscovery-agent.conf

    - name: Ensure latest ediscovery agent is installed
      package:
        name: ediscovery-agent
        state: latest

    - name: Ensure ediscovery agent is actually running
      service:
        name: ediscovery-agent
        state: started
      register: ediscovery_status

    - name: notify admins if agent was not already running
      slack:
        token: token/generatedby/slack
        msg: “{{ inventory_hostname }} had no running eDiscovery agent!”
      when: ediscovery_status.changed == true
```

Red Hat Ansible Engine kann in On-Premise- und Public Cloud-Infrastrukturen ausgeführt werden. Die Lösung wird sowohl auf Linux®- als auch auf Windows-Betriebssystemen unterstützt und gewährleistet so einen umfassenderen Zugriff auf elektronisch gespeicherte Unternehmensinformationen.

Während Ansible Engine die Ausführung von Playbooks verwaltet, bietet Red Hat Ansible Tower einen zentralen Überblick darüber, welche Playbooks ausgeführt wurden und in welcher Umgebung. Außerdem wird sofort angezeigt, welche Systeme noch analysiert werden müssen und in welchen Bereichen die Datenerfassung nicht gestartet wurde (Abbildung 1).

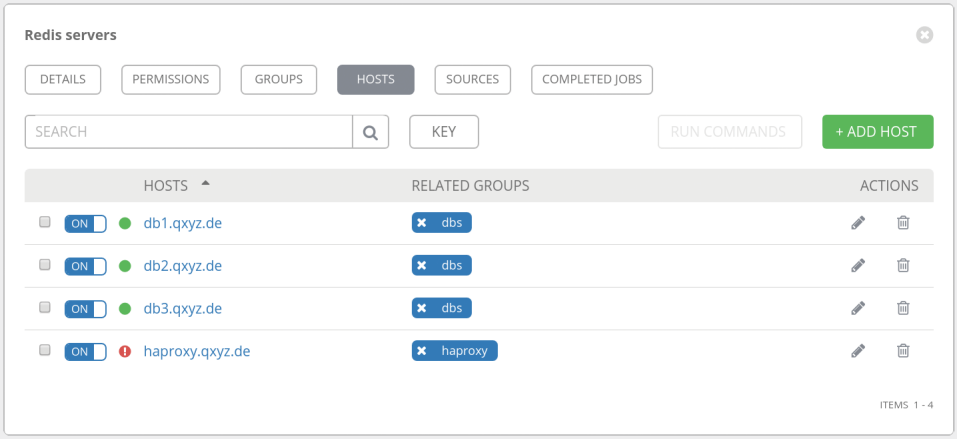

Abbildung 1. Red Hat Ansible Tower bietet eine zentralisierte Playbook-Schnittstelle

Auch wenn E-Discovery-Tools nicht automatisiert werden können – mit der Automatisierungs-Engine an sich können Sie das Ziel teilweise schon erreichen. Ansible kann beispielsweise Ressourcen Tags zuweisen und anschließend eine Zuordnung der physischen Ressourcenstandorte in einer Konfigurationsmanagement-Datenbank (CMDB) speichern, um die Datenhoheit im Sinne der DSGVO zu gewährleisten.

```
- name: ensure given files are not present anywhere
  hosts: all


  tasks:
    - name: get list with all important files
      win_find:
        path: \Users
        recurse: True
        patterns: ['*.doc','*.docx','*.xls','*.xlsx','*.pdf']
      register: all_files


    - name: Submit file list to CMDB via REST
      win_uri:
```

```
      url: “https://your.cmdb.example.com/rest/api/2/{{ inventory_hostname }}/files”
      method: POST
      body: “{{ all_files.files|map(attribute=’path’)|list() }}”
      body_format: json
```

USE CASE 2: SCHUTZ VERTRAULICHER DATEN ZUR DURCHSETZUNG KONTINUIERLICHER COMPLIANCE AUTOMATISIEREN

Da in der DSGVO die spezifischen Tools und Methoden nicht vorgeschrieben werden, die IT-Organisationen zur Aufrechterhaltung der Compliance verwenden müssen, gibt es je nach Risikobewertung verschiedene Möglichkeiten, wie Sie Ihre vertraulichen Daten schützen können. In machen Fällen sind unter Umständen erweiterte Schutzkonzepte wie Verschlüsselung erforderlich. In einem solchen Szenario ist die Automatisierung für eine erfolgreiche Implementierung von großer Bedeutung.

Ansible kann die Geräteverschlüsselung auf alle Maschinen anwenden, die bestimmte DSGVO-Kriterien im Bestand erfüllen. Im folgenden Playbook führt Ansible die Aufgabe ohne native Integration mit Drittanbietertools aus:

```
- name: ensure given files are not present anywhere
  hosts: all

  tasks:
  - name: check if device is available
    stat:
      path: /dev/mapper/lukscrypt
    register: stat_cryptdata

  - name: decrypt device if necessary
    shell:
      echo -n “{{ luks_pwd }}”|cryptsetup luksOpen /dev/md/0 lukscrypt
    when: stat_cryptdata.stat.exists == False

  - name: mount crypted device
    mount:
      path: /data
      src: /dev/mapper/lukscrypt
      state: mounted
      opts: noauto
```

Unabhängig von den verwendeten Compliance-Methoden müssen Unternehmen ihre fortlaufende Compliance unter Beweis stellen. Automatisierung in Verbindung mit Managementlösungen mit Selbstreparaturfunktionen, wie Red Hat Insights, bietet eine Echtzeiteinschätzung geschützter Systeme und eine automatisierte Fehlerbehebung für nicht konforme Szenarios.

In Abbildung 2 wurde von Red Hat Insights eine Sicherheitslücke erkannt, die durch die Ausführung eines Ansible Playbooks korrigiert werden kann. Das Playbook wird automatisch generiert. Anschließend wird es zum Herunterladen und zur manuellen Ausführung in den betroffenen Zielen zur Verfügung gestellt. Alternativ kann es in Ansible Tower importiert und zentral ausgeführt werden.

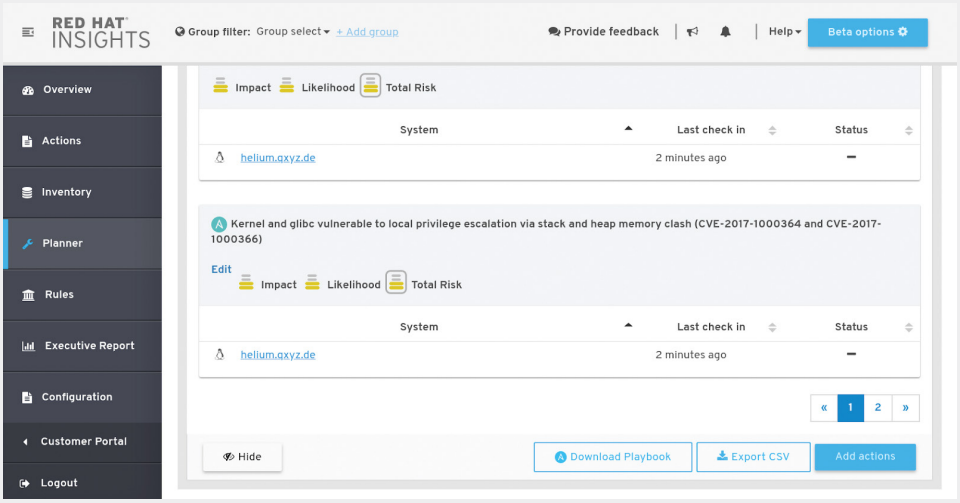

Abbildung 2. Erkennung einer Sicherheitslücke mit Red Hat Insights

USE CASE 3: BESEITIGUNG NICHT KONFORMER DATEN AUTOMATISIEREN

Sobald vertrauliche Daten erkannt, zugeordnet und geschützt wurden, können Sie alle anderen nicht konformen Daten löschen. Diese Aufgabe kann in großem Maßstab ausgeführt werden, indem Sie spezielle Playbooks schreiben, die von Ansible Engine je nach Bedarf auf Zielsystemen ausgeführt werden.

Die Automatisierung ist in einem solchen Szenario besonders hilfreich, da nicht konforme Daten möglicherweise auf Backup-Medien und in Offline-Storage gespeichert sind, deren manuelle Verarbeitung extrem ressourcenintensiv ist.

Beispiel: Ansible kann ein Playbook ausführen, das auf Mount-Server zugreift und vorübergehend ein definiertes Gerät mountet, und sicherstellen, dass alle Dateien aus einer bestimmten Liste nicht vorhanden sind. Abschließend kann das Playbook einen Bericht mit der Liste der gelöschten Dateien per E-Mail senden:

```
- name: ensure given files are not present anywhere
  hosts: backup-servers
  become: yes

  tasks:
    - name: mount backup dirs
      mount:
```

```
      path: /mnt/backup
      src: /dev/dm0
      fstype: xfs
      state: mounted

  - name: ensure files from forbidden list are deleted
    file:
      name: "{{ item }}"
      state: absent
    with_items:
      - "{{ lookup('file', 'forbiddenfiles.txt').split() }}"
    register: found_files

  - name: send report of deleted files via mail
    mail:
      host: smtp.gmail.com
      port: 587
      username: username@gmail.com
      password: "{{ secret_from_vault }}"
      to: Backup Reporting <backup.reporting@example.com>
      subject: Backup file deletion report
      body: "System {{ ansible_hostname }} deleted the files {{ found_files.results |
selectattr('changed')|map(attribute='item')|list() }}"
    when: found_files.changed == true

  - name: umount backup dirs
    mount:
      path: /mnt/backup
      state: unmounted
```

WEITERE INFORMATIONEN

Die automatisierten Prozesse in den drei beschriebenen Use Cases können in einem Master Playbook zusammengefasst und anschließend manuell oder automatisch, ad hoc oder regelmäßig, für ein neues IT-System ausgeführt werden, das in Ihrer IT-Umgebung bereitgestellt ist.

Red Hat Ansible Automation kann in zahlreichen weiteren Compliance-Szenarios eingesetzt werden, wie bei der automatisierten Bereitstellung von Kundendaten bei der Ausübung des Auskunftsrechts durch die betroffene Person (gemäß Art. 15 DSGVO), bei der Löschung von Kundendaten bei der Ausübung des Rechts auf Löschung (oder des „Rechts auf Vergessenwerden“) durch die betroffene Person (gemäß Art. 17 DSGVO) oder bei dem automatisierten Export von Kundendaten in einem gewünschten Format bei der Ausübung des Rechts auf Datenübertragbarkeit durch die betroffene Person (gemäß Art. 20 DSGVO)

Informationen zu den ersten Schritten mit Red Hat Ansible Automation finden Sie auf folgender Website: redhat.com/de/technologies/management/ansible/get-started.

Benötigen Sie Hilfe bei der Entwicklung einer Automatisierungsstrategie für Compliance? Starten Sie jetzt mit Red Hat Consulting unter https://www.redhat.com/de/services/consulting.

Weitere Informationen zur DSGVO finden Sie in folgenden Ressourcen:

- EUR-Lex: Datenschutz-Grundverordnung
- Fragen und Antworten zum Europäischen Parlament: „New EU rules on data protection put the citizen back in the driving seat“
- Red Hat: EU-Datenschutz-Grundverordnung (DSGVO)

ÜBER RED HAT

Red Hat, weltweit führender Anbieter von Open Source Software-Lösungen für Unternehmen, folgt einem community-basierten Ansatz, um verlässliche und leistungsstarke Technologien in den Bereichen Linux, Hybrid Cloud, Container und Kubernetes bereitzustellen. Wir unterstützen Kunden bei der Integration neuer und bestehender IT-Anwendungen, der Entwicklung cloudnativer Anwendungen, der Standardisierung auf unserem branchenführenden Betriebssystem sowie der Automatisierung, Sicherung und Verwaltung komplexer Umgebungen. Dank unserer vielfach ausgezeichneten Support-, Training- und Consulting-Services ist Red Hat ein bewährter Partner der Fortune 500 Unternehmen. Als strategischer Partner für Cloud-Anbieter, Systemintegratoren, Anwendungsanbieter, Kunden und Open Source Communities hilft Red Hat Organisationen auf ihrem Weg in die digitale Zukunft.

EUROPA, NAHOST, UND AFRIKA (EMEA)
00800 7334 2835
de.redhat.com
europe@redhat.com

TÜRKEI
00800 448820640

ISRAEL
1 809 449548

VAE
8000-4449549

facebook.com/redhatinc
@RedHatDACH
linkedin.com/company/red-hat

de.redhat.com
#F12392_0518