RED HAT ANSIBLE Automation

redhat.

EBOOK

COME SUPPORTARE LA CONFORMITÀ AL GDPR ATTRAVERSO L'AUTOMAZIONE

SOMMARIO

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com

INTRODUZIONE

Nel maggio del 2018, l'Unione europea (UE) ha avviato il più grande cambiamento nell'ambito della regolamentazione della privacy dei dati degli ultimi 20 anni. Il Regolamento generale sulla protezione dei dati (GDPR) europeo ha coinvolto molti ruoli in ogni entità europea impegnata nell'elaborazione dei dati personali.

Le violazioni del GDPR sulla privacy possono essere complicate da rilevare, correggere ed evitare. Negli ambienti DevOps agili e altamente scalabili, la conformità potrebbe essere molto difficile da raggiungere senza l'automazione. Inoltre, gli strumenti attualmente in uso per raccogliere, aggregare e proteggere i dati potrebbero non disporre delle funzionalità richieste per garantire la conformità al GDPR. Tuttavia, potrebbero offrire interfacce di programmazione delle applicazioni (API) e altri metodi di accesso programmatico automatizzabili per supportare la conformità.

I team IT possono aiutare i responsabili della protezione dei dati a far fronte alle sfide legate alla conformità al GDPR in molti modi. Una piattaforma di automazione facile da utilizzare, caratterizzata da una gestione centralizzata e da un'architettura modulare adatta a diversi scenari di utilizzo può rappresentare un solido supporto al GDPR.

Red Hat® Ansible® Automation, una piattaforma di automazione open source di livello enterprise, può essere utilizzata, indipendentemente o con altri strumenti, per offrire le funzionalità indispensabili al fine di garantire la conformità. Tra queste, le attività automatizzate di individuazione e mapping dei dati, la protezione automatizzata dei dati sensibili, l'eliminazione automatica dei dati non conformi, la fornitura dei dati dei clienti in conformità al Diritto di accesso, la cancellazione dei dati dei clienti in conformità al Diritto all'oblio o l'esportazione automatica dei dati dei clienti in conformità al Diritto alla portabilità.

COS'È IL REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI (GDPR)?

Il GDPR è il frutto della riforma dell'Unione europea della normativa sulla privacy, che ha l'obiettivo di uniformare le varie regolamentazioni nazionali sulla privacy dei dati. Introduce gli obblighi che le aziende sono tenute a rispettare nell'ambito della raccolta, dell'utilizzo e dell'elaborazione dei dati personali.

Secondo quanto previsto dal GDPR, i dati personali possono essere elaborati in caso sussista almeno uno dei seguenti requisiti legali: l'interessato ha fornito il proprio consenso per l'elaborazione dei dati personali per uno o più scopi specifici, oppure nel caso in cui l'elaborazione si renda necessaria:

- Per l'esecuzione di un contratto di cui l'interessato è Parte o per l'adozione di misure in caso di richiesta da parte dell'interessato prima di sottoscrivere un contratto.
- Per ragioni di conformità agli obblighi legali a cui è sottoposto il titolare del trattamento.
- Per proteggere gli interessi vitali dell'interessato o di un'altra persona fisica.
- Per l'esecuzione di un'attività di pubblico interesse o per l'espletamento delle funzioni ufficiali in qualità di titolare del trattamento.
- Per la persecuzione di scopi legati a legittimi interessi del titolare del trattamento o di terzi, tranne nel caso in cui diritti fondamentali o di libertà dell'interessato prevalgano su tali scopi, caso che richiederebbe la protezione dei dati personali, in modo particolare se l'interessato è un bambino.

L'ambito del GDPR va oltre i confini territoriali dell'UE per includere organizzazioni che offrono servizi o beni a individui nell'UE o che stanno monitorando il comportamento di un individuo nell'UE.

Le società non conformi al GDPR possono ricevere sanzioni per un valore che può arrivare fino al 4% del fatturato annuo globale o a € 20 milioni, a seconda di quale cifra sia superiore.

QUALI SONO LE SFIDE CORRELATE AL GDPR?

Nel giugno del 2017, Gartner ha rilasciato due dichiarazioni piuttosto significative:

1. Il 25 maggio 2018, meno del 50% di tutte le organizzazioni risulteranno pienamente conformi al GDPR.
2. Entro il 2020, verrà emessa una sanzione di diversi milioni di euro per mancata osservanza del GDPR.[1]

Secondo Gartner, queste supposizioni si basavano sulla difficoltà nel rilevare, correggere ed evitare le violazioni della privacy, soprattutto in ambienti DevOps scalabili e agili.

- **Difficoltà nel rilevarle,** perché, spesso, i dati dei clienti vengono raccolti attraverso vari canali, su più aree geografiche e linee di business, su più infrastrutture (on premise, cloud e ibride) e i dati non vengono sempre aggregati tramite una strategia consolidata di gestione dei dati. La portata della questione rende difficile valutare quali dati siano disponibili, di legittimo interesse e abbastanza sensibili da dover essere protetti e quali sia necessario eliminare per garantire la conformità al GDPR.
- **Difficoltà nel correggerle,** perché le soluzioni dipendono dall'esecuzione di attività su larga scala correlate ai dati dei clienti, quali l'aggiunta di pseudonimi, token o protezione in caso di cancellazione. Nel momento in cui i sistemi di dati non dispongono delle funzionalità native per l'esecuzione di queste attività, l'opzione migliore è utilizzare le API esistenti e altri metodi di accesso programmatico ai dati.
- **Difficoltà nell'evitarle,** perché una conformità continua richiede cambiamenti significativi nel modo in cui i dati vengono acquisiti, ad esempio tramite un'aggregazione centralizzata dei dati, come i Data Lake, e un sistema per automatizzare le verifiche e i report correlati alla conformità.

Inoltre, l'UE non è mai stata molto prescrittiva nell'ambito degli strumenti e dei quadri normativi necessari per rispettare i requisiti di conformità. Le soluzioni più ovvie volte a garantire la conformità al GDPR sono rappresentate dagli strumenti di gestione della privacy, quali la gestione integrata del rischio, gli strumenti di gestione dei cookie e di controllo della privacy, tra cui gli strumenti di gestione del ciclo di vita dei dati e degli pseudonimi, come tokenizzazione o data masking. Tuttavia, per sostenere una conformità scalabile, questi strumenti devono essere automatizzati.

SUPPORTARE LA CONFORMITÀ AL GDPR CON RED HAT ANSIBLE AUTOMATION

L'automazione è una funzionalità versatile ed efficiente e può avere diverse applicazioni in ambito informatico, tra cui l'elaborazione, le infrastrutture di rete e di storage, la configurazione dei sistemi operativi, il provisioning di applicazioni multilivello e l'applicazione delle politiche sulla sicurezza e delle normative sulla conformità.

È molto probabile che il tuo team IT stia già usando uno o più strumenti di automazione per alcune di queste attività, o in quanto parte di iniziative strategiche come i processi DevOps. Più lo strumento di automazione è flessibile, più sarà facile da usare per garantire la conformità al GDPR.

Secondo Joerg Fritsch, direttore della ricerca del team Security and Risk Management Strategies di Gartner: "I professionisti tecnici possono supportare il programma GDPR attraverso la tecnologia, ottenendo processi ripetibili e scalabili".[2]

Red Hat Ansible Automation è una piattaforma di automazione caratterizzata da un linguaggio facile da imparare, funzionalità di gestione centralizzata efficienti e un'architettura modulare in grado di risolvere le questioni relative alla conformità al GDPR in più scenari.

1 "GDPR Clarity: 19 Frequently Asked Questions Answered." Gartner. 29 agosto 2017.

2 Fritsch, Joerg. "A Technical Solution Landscape to Support Selected GDPR Requirements." Gartner. Febbraio 2018.

ESEMPIO DI UTILIZZO 1: RILEVARE I DATI SENSIBILI AUTOMATIZZANDO L'INDIVIDUAZIONE E IL MAPPING DEI DATI

Persino il processo di individuazione dei dati, se scalabile, può costituire una sfida. Red Hat Ansible Automation può semplificare l'individuazione e il mapping delle informazioni archiviate elettronicamente (ESI), ad esempio attraverso l'utilizzo di prodotti di e-discovery in tutta l'infrastruttura IT.

Red Hat Ansible Engine è agentless e si collega ai sistemi di destinazione tramite Secure Shell (SSH). I team IT sono in grado di scrivere flussi di lavoro automatizzati o playbook Ansible che usino un linguaggio semplice per descrivere e indicare in che modo l'agente di e-discovery viene implementato ed eseguito sui sistemi di destinazione.

```
- 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 funziona su infrastrutture on premise e di cloud pubblico, supportando sia Linux® che Windows e garantendo così un accesso più ampio alle ESI.

Mentre Ansible Engine gestisce l'esecuzione dei playbook, Red Hat Ansible Tower offre una visualizzazione centralizzata di quali playbook sono stati eseguiti e in quale ambiente, fornendo una visibilità immediata di quali sistemi devono ancora essere analizzati e dove la raccolta dei dati non è stata avviata correttamente (Figura 1).

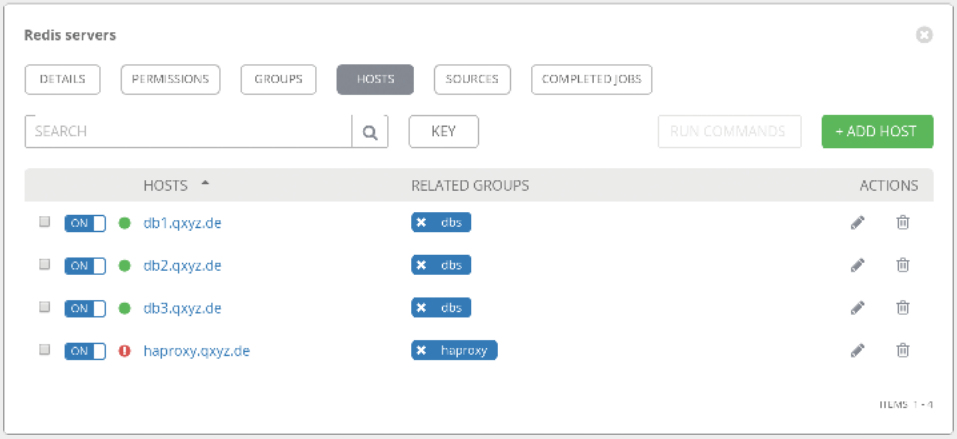

Figura 1. Red Hat Ansible Tower offre un'interfaccia centralizzata per la gestione dei playbook

Persino quando gli strumenti di e-discovery non possono essere automatizzati, il motore di automazione stesso può essere utilizzato per raggiungere parzialmente l'obiettivo. Ad esempio, Ansible può contrassegnare le risorse, quindi archiviare una mappa di posizioni fisiche delle risorse in un database di gestione della configurazione (CMDB) per indicare la sovranità dei dati per il GDPR.

```
- 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
```

ESEMPIO DI UTILIZZO 2: AUTOMATIZZARE LA PROTEZIONE DEI DATI SENSIBILI PER GARANTIRE LA CONFORMITÀ CONTINUA

Dato che il GDPR non indica gli strumenti specifici e i metodi che le organizzazioni IT devono seguire per essere conformi, i dati sensibili possono essere protetti in modi diversi, a seconda dell'esito della valutazione dei rischi. In alcuni casi, potrebbe essere necessario adottare degli approcci di protezione avanzata, come la crittografia. In questo scenario, l'automazione è fondamentale per ottenere un'implementazione corretta.

Ansible può applicare la crittografia del dispositivo a tutte le macchine il cui inventario soddisfi determinati criteri del GDPR. Nel seguente playbook, Ansible esegue l'attività senza disporre di un'integrazione nativa con strumenti di terzi:

```
- 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
```

A prescindere dai metodi utilizzati, le organizzazioni sono tenute a dimostrare continuità nel rispetto dei requisiti di conformità. L'automazione, unita alle soluzioni di gestione per la riparazione automatica come Red Hat Insights, fornisce una valutazione in tempo reale dei sistemi protetti e una correzione automatizzata degli scenari non conformi.

Nella Figura 2, Red Hat Insights ha identificato una vulnerabilità di sicurezza che può essere risolta eseguendo un playbook Ansible. Il playbook viene generato automaticamente e reso disponibile per il download e l'esecuzione manuale nelle destinazioni interessate. In alternativa, può essere importato in Ansible Tower per un'esecuzione centralizzata.

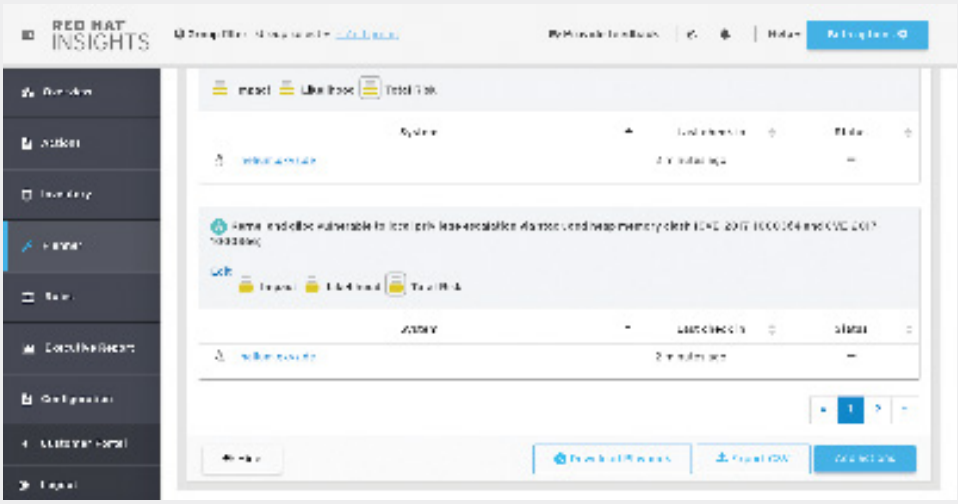

Figura 2. Identificazione di una vulnerabilità di sicurezza con Red Hat Insights

ESEMPIO DI UTILIZZO 3: AUTOMATIZZARE L'ELIMINAZIONE DEI DATI NON CONFORMI

Una volta identificati, mappati e protetti i dati sensibili, tutti i dati non conformi potranno essere rimossi. Questa attività può essere eseguita in modo scalabile scrivendo playbook specifici che verranno poi eseguiti da Ansible Engine sui sistemi di destinazione, in base alla necessità.

In questo scenario, l'automazione è un fattore chiave, in quanto i dati non conformi potrebbero essere archiviati su supporti di back up e tramite storage offline, ovvero processi caratterizzati da un utilizzo di risorse troppo elevato per poter essere elaborati manualmente.

Ad esempio, Ansible può eseguire un playbook che acceda ai mount server, monti temporaneamente un determinato dispositivo e verifichi che tutti i file di un elenco specifico non siano presenti. Infine, il playbook può inviare un report con l'elenco dei file eliminati tramite email:

```
- 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
```

SCOPRI DI PIÙ

I processi automatizzati dei tre esempi di utilizzo descritti possono essere uniti in un master playbook, quindi eseguiti manualmente o automaticamente, caso per caso o su base ricorrente, su qualsiasi nuovo sistema IT installato nel tuo ambiente.

Red Hat Ansible Automation può essere utilizzato ai fini di garantire la conformità in diversi altri scenari, come la fornitura automatica dei dati dei clienti in conformità al Diritto di accesso (Art. 15 del GDPR), la cancellazione dei dati dei clienti in conformità al Diritto all'oblio (Art. 17 del GDPR) o l'esportazione automatica dei dati dei clienti in un determinato formato in conformità al Diritto alla portabilità (Art. 20 del GDPR) su richiesta del soggetto interessato.

Per fare il primo passo con Red Hat Ansible Automation, visita https://www.redhat.com/it/technologies/management/ansible/get-started.

Vuoi sviluppare una strategia di automazione per migliorare la conformità? Fai il primo passo con Red Hat Consulting redhat.com/it/services/consulting.

Per ulteriori informazioni sul GDPR, consulta le seguenti risorse:

- EUR-Lex: General Data Protection Regulation
- European Parliament: Q&A: new EU rules on data protection put the citizen back in the driving seat
- Red Hat: EU General Data Protection Regulation (GDPR)

INFORMAZIONI SU RED HAT

Red Hat è leader mondiale nella fornitura di soluzioni software open source. Con un approccio basato sul concetto di community, distribuisce tecnologie come Kubernetes, container, Linux e hybrid cloud caratterizzate da affidabilità e prestazioni elevate. Red Hat favorisce l'integrazione di applicazioni nuove ed esistenti, lo sviluppo di applicazioni cloud-native, la standardizzazione su uno tra i principali sistemi operativi enterprise, e consente di automatizzare e gestire ambienti complessi in modo sicuro. I pluripremiati servizi di consulenza, formazione e assistenza hanno reso Red Hat un partner affidabile per le aziende della classifica Fortune 500. Lavorando al fianco di provider di servizi cloud e applicazioni, system integrator, clienti e community open source, Red Hat prepara le organizzazioni ad affrontare un futuro digitale.

ITALIA
it.redhat.com
italy@redhat.com

EUROPA, MEDIO ORIENTE,
E AFRICA (EMEA)
00800 7334 2835
it.redhat.com
europe@redhat.com

facebook.com/RedHatItaly
twitter.com/RedHatItaly
linkedin.com/company/red-hat

it.redhat.com
#F12392_0518