La guida essenziale per la conformità al GDPR

Brought to you by

Indice

Introduzione

Perchè è necessario riprogettare i sistemi in ottica “privacy by design”

Il 25 maggio 2018 entrerà in vigore il Regolamento generale sulla protezione dei dati dell’UE. Sostituirà ogni regolamento nazionale in materia di protezione dei dati all’interno dell’UE e chiunque operi nel mercato unico dovrà rispettarlo. Questo regolamento riguarderà anche le imprese extracomunitarie che conducono transazioni con clienti residenti nell’UE.

Secondo il GDPR, qualsiasi violazione dei dati personali dovrà essere segnalata entro 72 ore da quando se ne viene a conoscenza. La mancata segnalazione, oppure la mancata produzione di prove atte a smentire una negligenza, potrà portare a multe fino a 20 milioni di euro o al 4% del fatturato globale, a seconda di quale sia superiore.

Le misure necessarie per proteggere i dati aziendali nel loro complesso serviranno inoltre a mantenere sicuri i dati dei clienti. Lo stesso approccio di sicurezza degli endpoint a più livelli viene già da tempo consigliato da HP, e le imprese che l’hanno adottato risultano così già conformi al GDPR.

In questa pratica guida, esamineremo i componenti chiave del GDPR che i professionisti IT devono conoscere, e analizzeremo come un programma di sicurezza degli endpoint guidato dal dispositivo possa contribuire alla conformità prevista dalla legge di imminente applicazione.

Che cos'è il GDPR dell'UE

I punti chiave per l'IT

Il GDPR ha sostanzialmente due finalità: proteggere i diritti dei soggetti interessati dai dati e proteggere la privacy dei soggetti interessati dai dati all'interno dell'UE. Entrambi questi aspetti hanno importanti implicazioni tecnologiche.

Per i dettagli a livello burocratico, potete approfondire qui il testo completo. Per quanto concerne i responsabili decisionali IT, i punti salienti, da cui non è possibile prescindere, sono i seguenti:

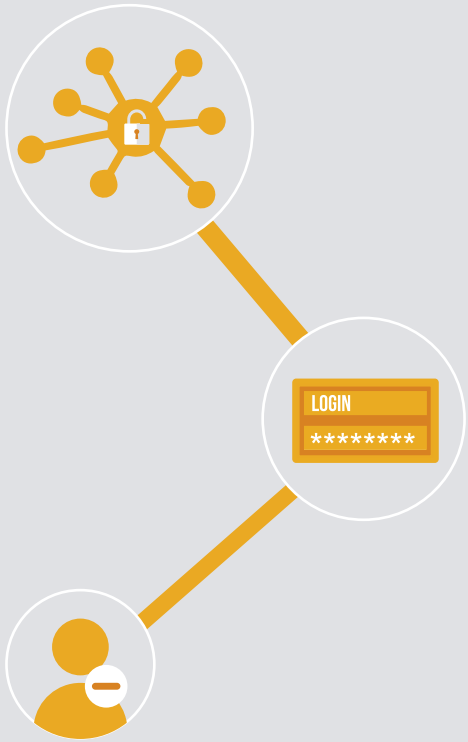
1. **Le violazioni devono essere segnalate entro 72 ore**
   Qualora si verificasse una violazione, questa dovrà essere segnalata entro 72 ore da quando se ne viene a conoscenza. Le sanzioni per la mancata segnalazione sono davvero ingenti (vedere "Quali sono le sanzioni per la mancata conformità?")

2. **Il diritto all'oblio**
   Ogni soggetto interessato da dati all'interno dell'UE ha il diritto di richiedere la rimozione di propri dati dai database delle imprese. Su richiesta, i dati dovranno essere cancellati, incluse tutte le copie.

3. **Il diritto alla portabilità dei dati**
   I residenti dell'UE hanno il diritto di controllare i propri dati. Su richiesta, i dati dovranno essere forniti in un formato accessibile agli utenti, che sono autorizzati a trasferirli a terzi

4. **Trasferimenti internazionali**
   Il trasferimento di dati personali a un'altra giurisdizione (al di fuori dell'UE) può essere effettuato solo con esplicito consenso e solo a "garanti" ritenuti "adeguati", oppure mettendo in atto misure di sicurezza aggiuntive[1]

5. **Privacy by design**
   Le organizzazioni devono adottare un approccio "privacy by design" che integri in maniera predefinita la sicurezza dei dati all'interno di prodotti, processi e servizi[2,3]



A chi si applica il GDPR?

Il GDPR si applica a qualsiasi azienda che raccolga e/o elabori dati personali di residenti dell'UE. Ciò include non solo le imprese che hanno sede in UE ma anche le organizzazioni con sede al di fuori dell'UE che operano al suo interno.

[1]https://iapp.org/news/a/top-10-operational impacts-of-the-gdpr-part-4-cross-border-data-transfers/ [2]Allen & Overy – The EU General Data Protection Regulation 2016
[3]http://www.computerweekly.com/news/450296306/10-key-facts-businesses-need-to-note-about-the-GDPR

Che cos’è il GDPR dell’UE

Che cosa si intende per “dati personali”?

Secondo il GDPR, i “dati personali” includono “qualsiasi dato che può essere utilizzato per identificare un individuo”.

Questi includono informazioni genetiche, intellettuali, culturali, economiche o sociali, oltre a quelle tradizionalmente considerate informazioni identificative.

Ciò può portare le organizzazioni precedentemente al di fuori del campo di applicazione della legislazione sulla protezione dei dati a ricadere nell’ambito del GDPR.

Quali sono le sanzioni per la mancata conformità?

La multa massima è di 20 milioni di euro o il 4% del fatturato globale, a seconda di quale tra le due sia superiore. Ciò si applica ai reati più gravi secondo il regolamento, come ad esempio, la mancata segnalazione di una violazione della sicurezza entro 72 ore da quando se ne viene a conoscenza.

Per i reati meno gravi il massimale è di 10 milioni di euro o il 2% del fatturato globale.

Lista di controllo delle procedure del GDPR

Nell’ambito del quadro della governance di dati, saranno necessarie procedure specifiche per:

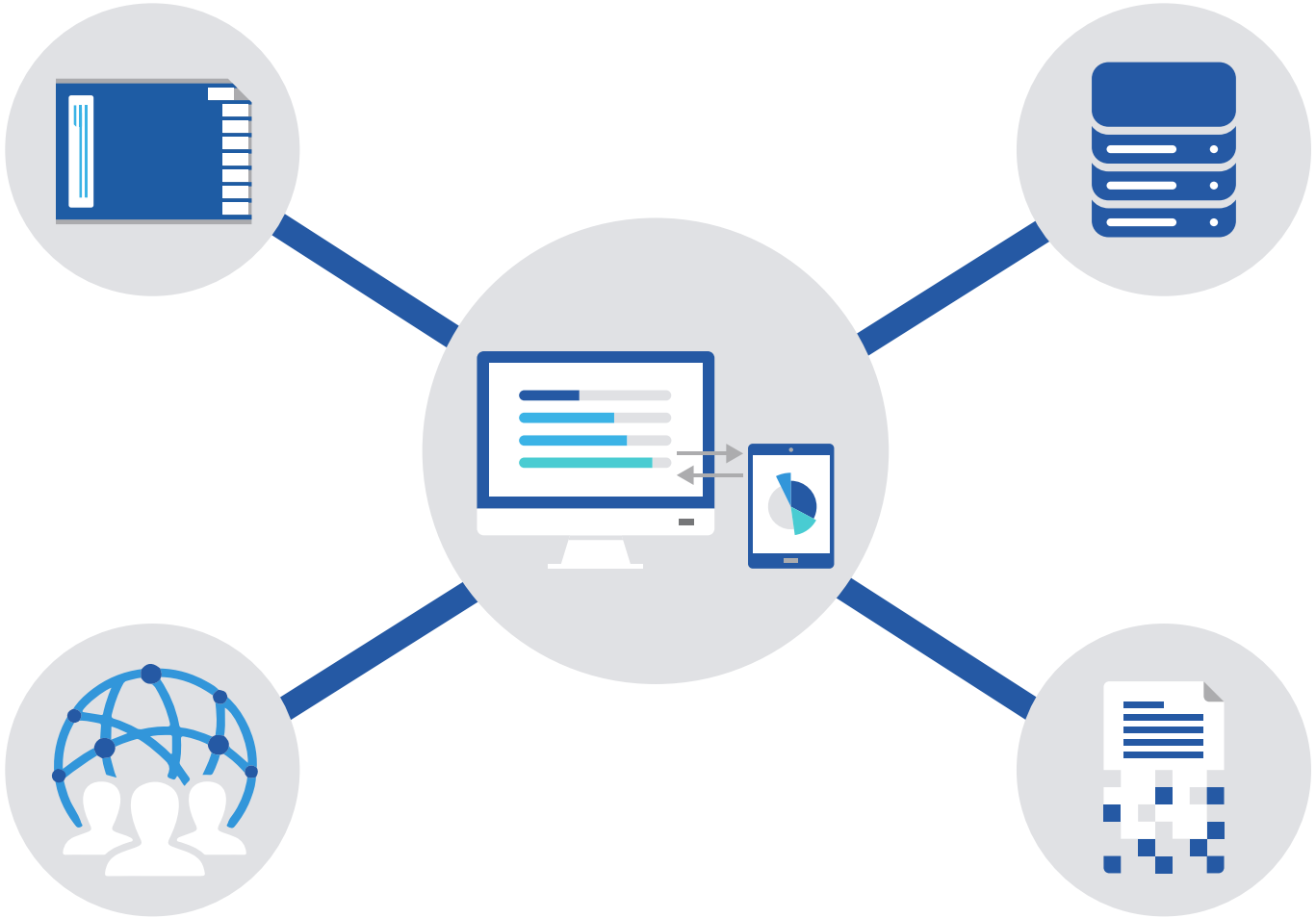
- Informare i soggetti interessati sul modo in cui i loro dati saranno raccolti, memorizzati ed elaborati
- Ottenere il consenso esplicito dei soggetti interessati a tale trattamento
- Fornire le informazioni sui soggetti interessati in un formato a loro accessibile
- Cancellare tutti i dati personali dei soggetti interessati, incluse le copie
- Trasferire i dati a un altro controller o processore di dati
- Trasferire i dati al di fuori dell’UE, seppur nell’ambito della stessa organizzazione

Sfide tecniche di conformità

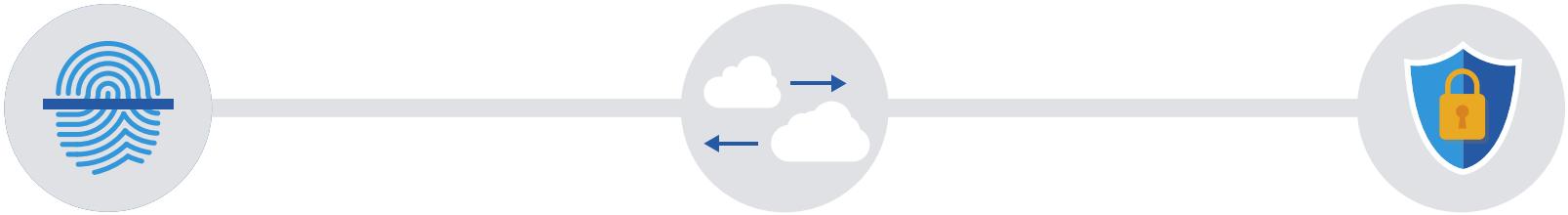
Le maggiori sfide del GDPR sono di natura tecnica.

Sarà necessario riprogettare i sistemi per consentire la portabilità dei datiin sicurezza e proteggere i dati di un individuo e il suo diritto all'oblio; questo richiede una mappa completa della posizione dei dati e l'accesso a questi ultimi a livello del dispositivo.

Poiché la minaccia della criminalità informatica aumenta di anno in anno, la tutela dei dati assume criticità crescente all'interno dei reparti IT.



Sfide tecniche di conformità



Tenere traccia dei dispositivi

Conformarsi alla portabilità dei dati e al diritto all'oblio richiede un esame dettagliato di tutti i dati personali di cui l'organizzazione è in possesso.

È necessario conoscere:

- Ogni dispositivo che contiene dati personali
- Ogni dispositivo che ha accesso ai dati personali

Questo è l'unico modo per garantire che sia possibile recuperare e/o cancellare i dati personali che l'azienda possiede.

Tenere traccia dei cloud

L'impresa europea media utilizza 608 app, una cifra che si stima sia sottovalutata del 90%. I dipendenti spesso utilizzano applicazioni cloud commerciali senza informarne il dipartimento IT.[4]

Per conformarsi al GDPR, l'utilizzo del cloud deve limitarsi ai servizi che si trovano:

- All'interno dell'UE e sono dunque conformi al GDPR
- Sotto la giurisdizione di un garante della protezione dei dati ritenuto "idoneo" dall'UE

Qualsiasi altra situazione potrebbe violare la normative internazionale in materia di trasferimento dei dati. È inoltre necessario sapere quali servizi cloud utilizzano i dipendenti, qualora il diritto all'oblio dovesse essere invocato.

Tenere i dati al sicuro

La minaccia della criminalità informatica si sta intensificando. Non da ultimo poiché l'utilizzo di reti e dispositivi personali non sicuri è in crescita.

Le violazioni sono pressoché inevitabili. L'UE ne è a conoscenza. Per evitare di incorrere in una multa consistente sarà necessario:

- Implementare uno strumento di monitoraggio degli eventi di sistema (Systems Incident Event Monitoring, SIEM) per segnalare una violazione entro 72 ore
- Implementare un sistema di sicurezza degli endpoint a più livelli per dimostrare la due diligence nel prevenire una violazione

Gli utenti devono inoltre essere consapevoli delle loro responsabilità nell'utilizzare dispositivi e reti non autorizzati.

[4]https://www.cloudindustryforum.org/content/cloud-and-eu-gdpr-six-steps-compliance

La minaccia della criminalità informatica

La criminalità informatica è una minaccia reale, presente e in aumento

L'82%

delle organizzazioni ha subito una minaccia/ violazione nei precedenti 12 mesi[5]

L'80%

dei professionisti IT ritiene che i crimini informatici aumenteranno nei prossimi tre anni[6]

Il 78%

delle aziende segnala un aumento degli attacchi malware negli ultimi cinque anni[7]

Il 60%

dei dirigenti IT ritiene che la criminalità informatica sovrasti le soluzioni di difesa a propria disposizione[8]

L'81%

delle aziende valuta la negligenza a livello di informazioni riservate come la più grande minaccia alla sicurezza informatica[9]

L'81%

dei dirigenti IT afferma che i dispositivi mobili della propria rete sono stati oggetto di attacchi malware[9]

Il 72%

afferma che l'utilizzo dei software cloud commerciali da parte dei dipendenti rappresenti per le aziende un rischio[9]

Il 69%

afferma che il BYOD (Bring Your Own Device, "porta il tuo dispositivo") è un rischio per la sicurezza

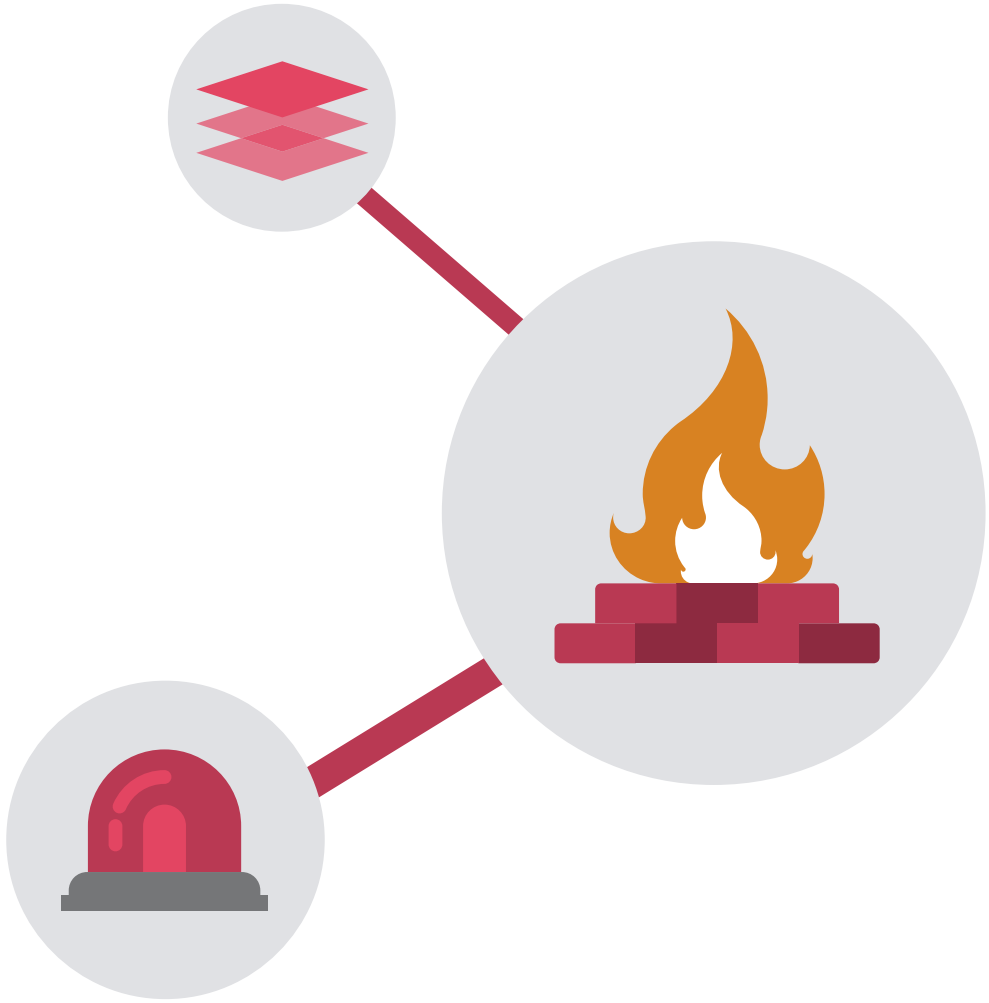
[5]HPI Printer Security Research 2016 (Spiceworks) [6]HP Printer Security Report 2015 [7] Ponemon 2016 State of the Endpoint Report [8]IBM CISO Assessment 2014 [9]Ponemon 2016 State of the Endpoint Report

Implementare la sicurezza degli endpoint

L'approccio di sicurezza degli endpoint a più livelli di HP

Un approccio alla sicurezza informatica focalizzato su firewall e antivirus, oggi non è più abbastanza. E forse non lo è mai stato. In uno studio di Damballa, il software antivirus ha impiegato sei mesi per identificare ed eliminare il 100% dei file maligni lanciati.[10]

HP ritiene che la sicurezza informatica debba essere multilivello, operante cioè a livello di rete, dispositivo e utente, con più soluzioni di protezione per ciascuno di essi. Il concetto di rilevamento e risposta deve essere preferito a quello di protezione e difesa. E tutto ha inizio dagli endpoint: sia a livello di dispositivo che di utente.



Controlli di sicurezza critici (CSC)

Il Centro per la sicurezza Internet (Center for Internet Security, CIS) ha definito 20 controlli di sicurezza critici (Critical Security Control, CSC) che sono stati riconosciuti a livello internazionale e sviluppati, perfezionati e convalidati dai principali esperti di sicurezza IT in tutto il mondo.

È possibile scaricare gratuitamente il documento completo nell'archivio CIS.

[10]https://www.damballa.com/time-to-fix-malware-strategies-2/

Sicurezza di rete

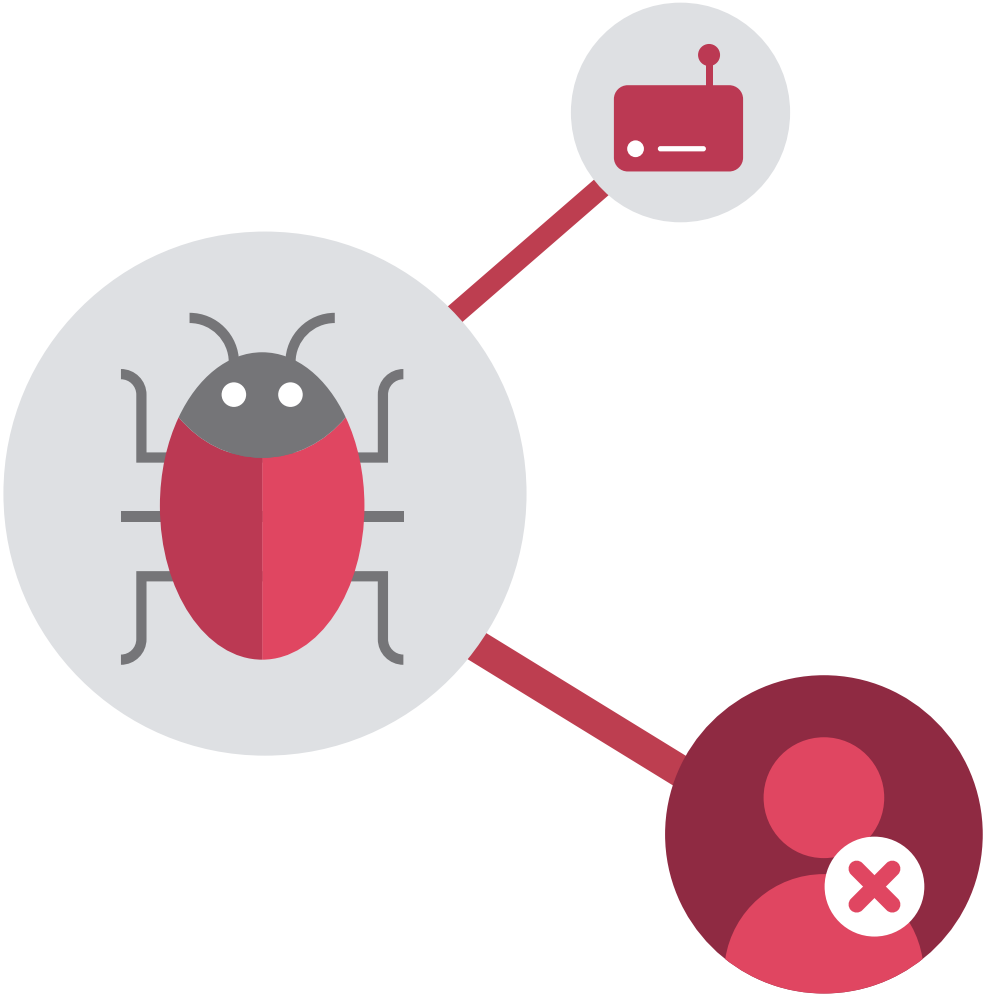
I principali attacchi informatici tendono a sfruttare un unico punto di accesso per accedere all'intera rete. La sicurezza a livello di rete deve pertanto basarsi sul prevenire tale azione.

- **Privilegi a livello di controllo amministrativo (CSC 5)**
  Restringere fino al minor numero di persone possibile, il totale delle risorse dotate di facoltà di cambiare le impostazioni di rete e le password.
- **Definire un accesso di controllo basato sulla "necessità di sapere" (CSC 14)**
  Ponderare il rischio di sicurezza rispetto alla sensibilità dei dati.
- **Limitazione e controllo delle porte di rete, dei protocolli e dei servizi (CSC 9)**
  Spegnere tutti i punti di accesso non necessari, virtuali e fisici, compresi i servizi FTP, Telnet e di stampa
- **Gestione, monitoraggio e analisi dei registri di controllo (CSC 6)**
  Esaminare regolarmente i registri di controllo per analizzare l'andamento del sistema e rilevare eventuali attività sospette
- **Valutazione e correzione continua della vulnerabilità (CSC 4)**
  Valutare continuamente l'ambiente per rilevarne la vulnerabilità e agire per correggere i risultati, riducendo al minimo le opportunità di violazione

Obiettivo ultimo di tali procedure è la costruzione di una rete suddivisa in più livelli in base alla sensibilità delle informazioni. Le richieste di accesso verranno valutate tenendo conto dei rischi per la sicurezza. Le informazioni più sensibili saranno rese inaccessibili a dispositivi, utenti e richieste provenienti da reti non sicure.[11]

[11] https://research.google.com/pubs/pub43231.html

Sicurezza di rete



Ogni dispositivo, aziendale o personale che sia, è una fonte di potenziale vulnerabilità. È necessario conoscere ogni telefono, tablet, computer portatile e desktop che abbia accesso ai dati aziendali.

- **Inventario di dispositivi autorizzati e non autorizzati (CSC 1)**
  Verificare ogni dispositivo che abbia accesso ai dati
- **Inventario di software autorizzati e non autorizzati (CSC 2)**
  Verificare ogni applicazione utilizzata sulla rete.
- **Soluzioni di difesa da malware (CSC 8)**
  Assicurarsi che ogni dispositivo disponga di antivirus e malware aggiornati. Garantire scansioni e aggiornamenti regolari

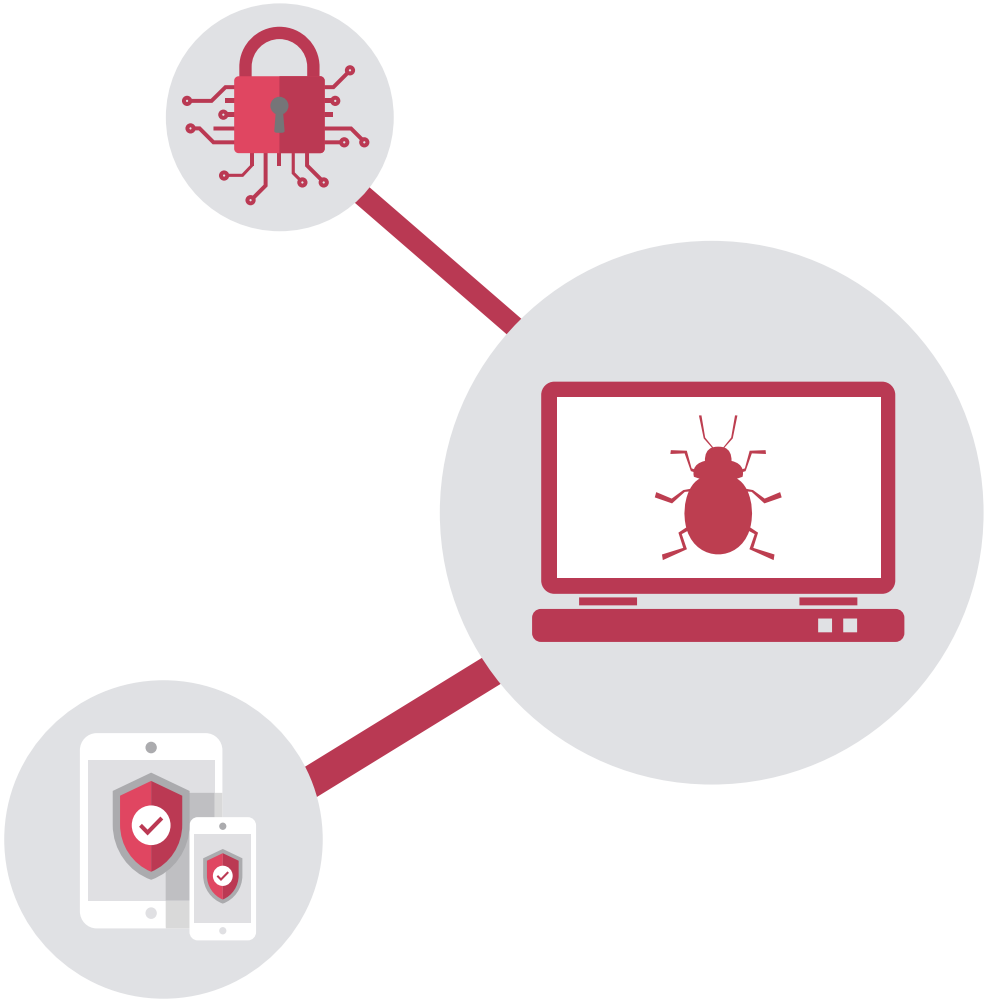
Device security

Inoltre, i dipartimenti IT devono considerare i seguenti controlli aggiuntivi:

- **L'autenticazione a più fattori**
  Assicurarsi che ogni dispositivo di lavoro sia sicuro. Potrebbe essere utile a questo scopo, optare per l'autenticazione biometrica unitamente alle password (vedere pagina 14: "Dispositivi di privacy by design")
- **Accesso remoto**
  Garantire l'accesso remoto ai dispositivi per recuperare o cancellare i dati personali, mettere in quarantena e terminare i processi, nonché arrestare e bloccare il dispositivo in caso di perdita o furto (vedere pagina 14: "Rilevamento e risposta")
- **Informare ogni dipendente sui protocolli e sulle procedure di sicurezza**
  Assicurarsi che ogni dipendente sia a conoscenza delle procedure di sicurezza e riconosca le proprie responsabilità in materia di sicurezza informatica, inclusa la segnalazione di attività sospette
- **Tenere corsi di formazione attiva sulla sicurezza informatica**
  Ospitare workshop, seminari, esercitazioni sul phishing, assicurandosi che tutti sappiano come evitare gli errori di base e come rimanere conformi al GDPR
- **Ridurre al minimo l'utilizzo di dispositivi/app personali**
  Scoraggiare l'utilizzo di dispositivi e app personali per scopi lavorativi. Una politica CYOD (Choose Your Own Device, "scegli il tuo dispositivo") completa e flessibile può essere d'aiuto

L'implementazione di un quadro di sicurezza come questo deve contribuire a mantenere il controllo sui dispositivi aziendali per facilitare l'applicazione della portabilità dei dati e del diritto all'oblio.

Per maggiori informazioni sull'approccio di sicurezza a più livelli di HP, leggete il nostro whitepaper la sicurezza comincia dagli endpoint.



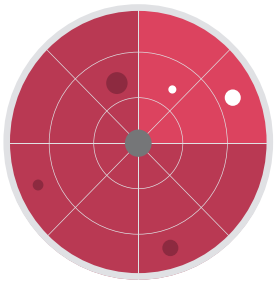
Perché ogni dipendente deve avere buone conoscenze informatiche

Il 58% delle minacce informatiche proviene da dipendenti, ex dipendenti e partner di fiducia.[12] Rendere sicuro ogni dispositivo significa anche rendere sicure le azioni del suo utente.

- Il Comitato nazionale democratico (Democratic National Committee, DNC) degli Stati Uniti è stato attaccato nel 2016 quando John Podesta ha fatto clic su un link di phishing erroneamente indicato come legittimo da un assistente[13]
- Foto di celebrità nude hanno invaso Internet nel 2014, dopo che il trentaseienne Ryan Collins ha ottenuto l'accesso al Cloud di Jennifer Lawrence[14]
- 68 milioni di password di Dropbox sono trapelate nel 2012 grazie a un dipendente che utilizzava la stessa password sia per i sistemi interni che per il suo profilo LinkedIn[15]
- Il Presidente Donald Trump continua a utilizzare un telefono standard Samsung Galaxy. Gli esperti non si chiedono se sia stato hackerato, ma piuttosto quante agenzie di intelligence straniere lo hanno già fatto[16]

[12]http://www.clearswift.com/sites/default/files/images/blog/enemy-within.pdf [13]https://www.theguardian.com/us-news/2016/dec/14/dnc-hillary-clinton-emails-hacked-russia-aide-typo-investigation-finds [14]http://www.forbes.com/sites/thomasbrewster/2016/03/16/icloud-hacking-jennifer-lawrence-fappening-apple-nude-photo-leaks/#45fed5d77b88 [15]https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach [16]https://www.theguardian.com/commentisfree/2017/feb/19/if-trump-hates-leaks-needs-to-give-up-phone

Rilevamento e risposta

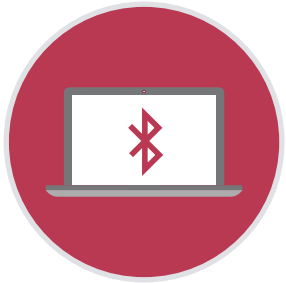


Rilevamento e risposta è il nome di un quadro di sicurezza informatica che riconosce la quasi impossibilità di una prevenzione totale.

Ciò che conta è essere a conoscenza della violazione (rilevamento) e agire immediatamente (risposta).

Sono disponibili prodotti software che trasformano ogni dispositivo in un sensore in tempo reale e che consentono all'amministratore di rispondere, ad esempio, spegnendo i dispositivi, mettendo in quarantena i file e cancellando i dati.

Dispositivi privacy by design



I dispositivi HP sono realizzati tenendo conto, sin dalla farse di progettazione, della privacy by design.

Le funzioni di sicurezza includono il primo BIOS con riparazione automatica al mondo, il blocco Bluetooth automatico (che blocca il dispositivo quando ci si allontana) e le schermate di privacy integrate.

Tali funzioni di per sé non garantiscono la conformità al GDPR ma, inserite in un sistema di procedure corretto, contribuiscono a soddisfare le richieste del decreto stesso.

Prepararsi al GDPR

Misure pratiche da intraprendere ora

Il GDPR entrerà in vigore il 25 maggio 2018. C'è ancora tempo per prepararsi ma, com'è risaputo, c'è molto da fare.

Per prima cosa, bisogna **verificare la situazione attuale relativa ai dati**. Valutare dove sono memorizzati, dove vengono copiati e chi ha accesso a tali dati. Se si utilizzano soluzioni cloud, scoprire dove sono basati i server e se sono conformi al GDPR. Lo stesso vale per qualsiasi SaaS o altra organizzazione partner con cui si lavori e condividano i dati. Questa prima analisi consentirà di avere un'idea chiara delle modifiche necessarie per essere a norma con quanto richiesto dalla legge.

Progettare la propria politica sui dati. Includere procedure e protocolli dettagliati su dove sono memorizzati i dati, su chi vi ha accesso e produce copie al di fuori dell'azienda oppure oltre i confini nell'ambito di una multinazionale.

Includere procedure per il recupero e la cancellazione dei dati personali comunicandole a tutta l'azienda. Tenere corsi di formazione e sottolinearne l'importanza.

Progettare la propria politica sulla sicurezza. Creare un nuovo quadro di sicurezza informatica che funzioni dal punto di vista degli endpoint, improntati su standard di rilevamento e risposta. Se necessario, revisionare la politica sui dispositivi, o investire in nuove tecnologie. Solo il 36% dei dirigenti IT ritiene di avere un budget sufficiente per la sicurezza degli endpoint.[17] Le sanzioni del GDPR potrebbero essere finalmente la chiave per ottenere l'interesse dell'alta dirigenza.

[17]Ponemon 2016 State of the Endpoint Report

Prepararsi al GDPR

GDPR checklist

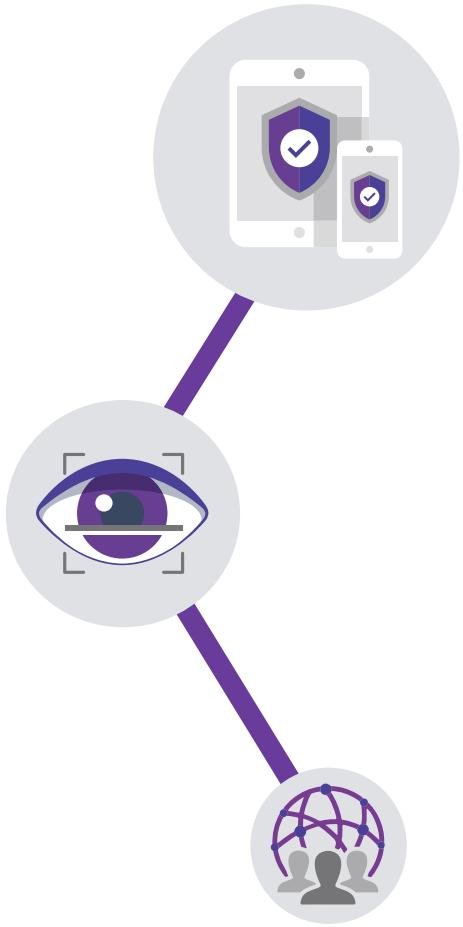
5 passi chiave per conformarsi al GDPR

1. Se necessario, nominare qualcuno che sia responsabile dei dati, un Data Protection Officer (DPO)
2. Condurre un'analisi completa dei dati, inclusa l'idoneità dei provider di cloud e SaaS in riferimento al GDPR
3. Creare un nuovo quadro per la governance dei dati, incluse le procedure per la portabilità dei dati e il diritto all'oblio
4. Creare un nuovo quadro di sicurezza informatica, implementando la sicurezza degli endpoint a più livelli
5. Comunicare politiche e protocolli a tutta l'azienda

Device Security Checklist

6 passi chiave per proteggere gli endpoint

1. Verificare tutti i dispositivi autorizzati e non autorizzati che hanno accesso a dati personali
2. Se necessario, investire in dispositivi nuovi e più sicuri
3. Implementare diritti di accesso e cancellazione remoti per i dati aziendali sui dispositivi
4. Implementare una politica di analisi e di aggiornamento del software da ripetere a intervalli regolari
5. Implementare software di rilevamento e risposta in tempo reale
6. Formare i dipendenti sulla sicurezza informatica



Calendario di sicurezza degli endpoint

Una cronologia di base per l'implementazione della sicurezza degli endpoint in vista del GDPR

2017

Maggio

Nominare il responsabile di progetto incaricato di implementare la sicurezza degli endpoint

Giugno

Condurre un'analisi delle politiche, delle pratiche e dei dispositivi di sicurezza attuali

Luglio

Considerare i requisiti e le politiche dei dispositivi per la sicurezza degli endpoint (CYOD/BYOD e così via)

Agosto

Considerare le soluzioni software di rilevamento e risposta alla sicurezza

Settembre

Progettare un sistema di accesso a più livelli e stratificato per i dati aziendali

Ottobre

Progettare cloud pubblici/privati per consentire l'accesso appropriato ai dati esterni

Novembre

Progettare un programma di formazione degli utenti, incluse pratiche regolari di riconoscimento del phishing

Dicembre

Comunicare nuove politiche sulla sicurezza al resto dell'azienda

2018

Gennaio

Implementare nuove architetture di dati sui cloud pubblici/privati

Febbraio

Implementare nuove politiche di sicurezza e tutela dei dati sui dispositivi

Marzo

Implementare soluzioni software di rilevamento e risposta

Aprile

Condurre la formazione sulla sicurezza degli utenti, incluse le politiche relative al GDPR

Maggio

Il GDPR entra in vigore

Riassunto

Il GDPR non è poi così lontano

Se siete lungimiranti, la vostra organizzazione sta già mettendo in pratica gran parte di quanto contenuto nei regolamenti: si tratta principalmente di trasformare in procedure consolidate ciò che dovrebbe già essere prassi.

E se avete condotto affari in più Paesi dell'UE, potreste esservi già imbattuti in alcune delle misure più severe contenutevi.

Le misure di sicurezza che raccomandiamo di mettere in atto per conformarsi al GDPR sono misure che aiutano a prevenire qualsiasi violazione, il cui impatto si può rivelare incredibilmente costoso per un'organizzazione. Secondo le ultime cifre, il governo del Regno Unito ha stimato che le aziende britanniche hanno perso 21 miliardi di sterline in un solo anno, per riprendersi dagli attacchi informatici, una cifra che si prevede in deciso aumento.[18]

Inoltre, molte delle misure necessarie per una sicurezza veramente efficace contribuiscono anche a rispettare altri aspetti del GDPR. Limitare l'accesso ai dati a determinati utenti, dispositivi o reti non solo riduce al minimo i rischi relativi ai dati, ma rende anche più semplice la tracciabilità dei dati personali e quindi la conformità alla portabilità dei dati e al diritto all'oblio, per non parlare dei trasferimenti internazionali degli stessi.

Per HP, la sicurezza è sempre stata una priorità: la privacy by design ha caratterizzato le scelte produttive e di progettazione da anni. Ora che è necessaria, piuttosto che auspicata, siamo in grado, grazie alla nostra esperienza, di aiutarvi ad adottare nel modo più efficace, lo stesso approccio.

Per sapere di più su come HP e i nostri prodotti possono contribuire a rispettare il GDPR, visitate **la nostra pagina "Privacy by design".**

[18]https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the cost-of-cyber-crime-full-report.pdf