Proofpoint Threat Response e GDPR

Garantire la conformità grazie all'automazione della sicurezza e alle buone norme in materia di privacy dei dati

VANTAGGI PRINCIPALI

Adozione di buone norme di sicurezza

- Neutralizza e minacce mirate in modo più rapido ed efficace.
- Alleggerisci il carico di lavoro del team IT grazie alla risposta automatica agli incidenti.
- Riduci il calo di concentrazione causato dall'elevato numero di allarmi.
- Acquisisci e assegna le priorità ai dati che provengono da dispositivi di sicurezza diversi.
- Ottieni una visione contestuale dettagliata di tutte le minacce.

Conformità al GDPR

- Impedisci la condivisione di dati personali con terze parti esterne all'azienda.
- Assicura l'integrazione con i sistemi di controllo interni.
- Aggiungi Proofpoint Threat Response ai record interni di elaborazione dati.
- Dimostra la conformità con il supporto di Proofpoint.

Oggi, la maggior parte delle aziende di successo utilizza tecnologie di automazione per gestire gli incidenti di sicurezza. Cosa ci dice questa tendenza? Quali fattori dovresti prendere in considerazione se stai pensando di automatizzare i sistemi di sicurezza per essere conforme con le normative, seguire le buone norme e e godere di benefici a lungo termine?

AUTOMAZIONE DELLA RISPOSTA AGLI INCIDENTI: UNA NECESSITÀ

L'attuale panorama della sicurezza informatica esige una risposta rapida. Purtroppo, i team della sicurezza devono affrontare molte sfide che impediscono loro di rispondere alle minacce mirate in modo rapido ed efficace. Ecco alcuni esempi:

- **Carenza di personale:** la risposta agli incidenti può essere un processo lento e molto impegnativo. Alcune attività sono dispendiose in termini di tempo e spesso creano colli di bottiglia. Inoltre, ripetere gli stessi compiti per ogni incidente può portare a un sovraccarico del vostro di team di sicurezza, già sotto pressione.
- **Calo di concentrazione a fronte di un elevato numero di allarmi:** maggiore è il numero di dispositivi di sicurezza su cui si fa affidamento, più aumentano gli allarmi. Spetta poi al tuo team della sicurezza assegnare manualmente le priorità a tali allarmi. Qual è il problema correlato? Questo modo di operare è soggetto all'errore umano. E spesso i veri incidenti rischiano di essere trascurati.
- **Dispositivi e dati di sicurezza eterogenei:** l'analisi degli incidenti si basa su informazioni che provengono da molteplici fonti non collegate tra loro. Ogni singolo dato fa parte dell'equazione. Come la maggior parte delle aziende, anche la tua si trova ad affrontare un crescente numero di minacce mirate, e rispondere entro pochi minuti è fondamentale. Purtroppo, troppe informazioni eterogenee possono rallentare il processo di risposta agli incidenti.

Le soluzioni di orchestrazione, automazione e risposta agli incidenti di sicurezza (SOAR, Security Orchestration, Automation and Response) possono aiutare a risolvere questi problemi. Sono in grado di acquisire allarmi provenienti da diverse fonti e di integrare le attività di automazione della risposta agli incidenti. L'utilizzo di una soluzione SOAR permette di risparmiare tempo, ma anche di limitare o ridurre il numero di personale a tempo pieno necessario per gestire gli incidenti di sicurezza automatizzando il processo di risposta. Ciò contribuisce a ridurre il tempo medio per rispondere, contenere e applicare le misure correttive.

Proofpoint Threat Response è una soluzione SOAR che elimina le attività manuali e l'incertezza associate alla gestione degli incidenti. Ciò consente al team della sicurezza di porre rimedio alle minacce in modo più rapido ed efficace. Proofpoint Threat Response acquisisce gli allarmi da fonti diverse, li arricchisce e li confronta automaticamente con dati contestuali essenziali forniti dalle informazioni sulle minacce di Proofpoint, il tutto in pochi secondi. Inoltre, fornisce informazioni complete sugli attacchi (chi, cosa e dove), mappa gli indirizzi IP degli utenti e fornisce informazioni sulle minacce esterne, come i feed STIX e TAXII standard. Ciò consente agli analisti di effettuare rapidamente il triage degli incidenti di sicurezza. In base al contesto e alle informazioni raccolte e analizzate, Proofpoint Threat Response presenta una visione contestuale completa di tale minaccia. Gli analisti possono così applicare misure di risposta automatizzate, come ad esempio:

- Rimuovere le email consegnate dalle caselle di posta degli utenti
- Aggiungere utenti a gruppi con autorizzazioni limitate
- Aggiornare le liste di blocco dei firewall e dei filtri web
- Contenere le minacce bloccandole/mettendole in quarantena su Microsoft Exchange, firewall, soluzioni per il rilevamento e la risposta alle minacce sui terminali (EDR, Endpoint Detection and Response), gateway web, Microsoft Active Directory, soluzioni di controllo dell'accesso alla rete (NAC, Network Access Control), ecc.

PRIVACY DEI DATI E OPERAZIONI DI SICUREZZA

GDPR e liceità del trattamento dei dati

Come previsto dal regolamento generale sulla protezione dei dati (GDPR) dell'Unione europea, il trattamento dei dati personali è un compito legittimo dei responsabili del trattamento. Ciò è particolarmente vero nelle aree in cui i dati personali sono necessari per garantire la sicurezza della rete e dell'informazione. Il trattamento dei dati personali è altresì legittimo nell'ambito della prevenzione di atti illeciti o dolosi che possono compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati personali, memorizzati o trasmessi. Tali "interessi legittimi" sono definiti nell'articolo 6 del GDPR "Liceità del trattamento". Un interesse legittimo è quindi confermato dalla legge. Ma esclusivamente se si è in grado di giustificare la necessità del trattamento. Inoltre, il trattamento deve rispettare i principi di proporzionalità e sussidiarietà. Queste eccezioni all'uso dei dati personali ai fini della sicurezza informatica sono definite nell'articolo 6, paragrafo 1, lettera f) del GDPR e nel considerando 49 del GDPR.

Quando si tratta di conformità al GDPR, ampliare e proteggere l'infrastruttura con servizi di sicurezza come Proofpoint Threat Response è un grande vantaggio. Componente fondamentale di ogni architettura IT moderna, Proofpoint Threat Response consente il trattamento dei dati per mezzo di architetture di sicurezza esterne, come ad esempio un fornitore di informazioni sulle minacce o servizi di sicurezza. Proofpoint Threat Response non condivide alcun dato con terzi, ma li utilizza solo per gli scopi concordati e descritti nel contratto di servizio stipulato tra l'utente e Proofpoint. Inoltre, Proofpoint Threat Response è disponibile solo per l'implementazione in locale, senza alcun trasferimento di dati all'esterno per impostazione predefinita.

Aggiunta di Proofpoint Threat Response ai registri delle attività di trattamento

Per essere conferme al GDPR, la soluzione deve anche rispettare i principi di parametrizzazione e di integrazione con altri sistemi. È possibile aggiungere Proofpoint Threat Response ai record interni di trattamento dei dati, in conformità con le disposizioni dell'articolo 30 del GDPR "Registri delle attività di trattamento".

Scambio interno di dati personali

L'articolo 47 del GDPR "Norme vincolanti d'impresa" permette la condivisione a livello internazionale di informazioni interne a un gruppo di entità situate in diversi paesi. Queste regole aziendali devono includere tutti i principi fondamentali della privacy dei dati e i diritti applicabili per assicurare un'adeguata protezione dei trasferimenti o delle categorie di trasferimenti di dati personali.

Per garantire la conformità al GDPR, è indispensabile un sistema di controllo interno (Internal Control System, ICS). È quindi necessario implementare un sistema di questo tipo. Un sistema ICS per essere conforme deve essere costituito da un sistema di controllo interno e da un sistema di monitoraggio. Il sistema di controllo permette di controllare le attività dell'azienda; inoltre, garantisce la corretta registrazione delle transazioni commerciali e il rispetto dei principi del GDPR.

SCAMBIO DI DATI CON TERZE PARTI[1]

Per garantire un livello di protezione adeguato, il GDPR consente alle aziende di ricorrere ad esperti, strumenti o servizi esterni a supporto delle misure di sicurezza interne. Esistono severe normative GDPR per garantire che questi fornitori terzi (responsabile del trattamento) rispettino il livello di protezione dei dati della tua azienda. Queste sono definite nell'articolo 28 “Responsabile del trattamento”. Il titolare del trattamento deve reclutare solo responsabili del trattamento in grado di garantire che tutte le misure tecniche e organizzative applicate soddisfino appieno i requisiti del GDPR. I responsabili del trattamento dei dati devono assicurare la tutela dei diritti dell’interessato.

Per aiutarti a soddisfare tale rigido requisito e garantire così la conformità della tua azienda, Proofpoint fornisce diversi documenti da conservare per tutti i prodotti correlati. Tra questi, sono inclusi i contratti per il trattamento dei dati da conservare nel registro delle attività di trattamento.

Concepito tenendo ben presenti le buone norme del settore e dei requisiti in materia di conformità, Proofpoint Threat Response automatizza e velocizza le attività di risposta agli incidenti. Inoltre, aiuta a garantire che l'utilizzo dei dati personali in un contesto di sicurezza sia pienamente conforme al GDPR. Come vantaggio ulteriore, Proofpoint fornisce la documentazione necessaria per aiutarti a dimostrare la conformità.

1 Quando si configurano scambi di dati o servizi esterni (esempio: Proofpoint Targeted Attack Protection).

APPROFONDISCI

Per maggiori informazioni visita **proofpoint.com/it**.