

Kaspersky: leader nella valutazione indipendente della trasparenza e della responsabilità dei fornitori di sicurezza informatica

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Kaspersky ha pubblicato *Protection beyond detection: Why trust and transparency decide your cybersecurity future*, un nuovo white paper basato su una valutazione indipendente della trasparenza e della responsabilità di 14 fornitori leader nel settore della sicurezza informatica. Dallo studio, Kaspersky emerge come uno dei fornitori più trasparenti analizzati, superando costantemente gli standard di settore in materia di trattamento dei dati, affidabilità della catena di fornitura e capacità di verifica da parte dei clienti.

Lo studio indipendente *Transparency Review and Accountability in Cyber Security* (Trasparenza, revisione e responsabilità nella sicurezza informatica), su cui si basa il white paper di Kaspersky, è stato commissionato dalla Wirtschaftskammer Österreich (WKO) e condotto da MCI | The Entrepreneurial School® ed esperti legali, in collaborazione con AV-Comparatives. La ricerca valuta i fornitori sulla base di un'ampia gamma di criteri di trasparenza e responsabilità e rileva che, sebbene la conformità di base sia diffusa, molte pratiche verificabili volte a rafforzare la fiducia restano ancora poco adottate nel settore.

La valutazione ha individuato diversi fattori chiave di differenziazione. Kaspersky è risultata uno dei soli tre fornitori, su 14 valutati, a offrire ai propri clienti l'accesso a Centri di Trasparenza, dove è possibile esaminare in modo indipendente il codice sorgente, le pratiche di gestione dei dati e i processi di aggiornamento. Tra questi, Kaspersky si distingue per l'offerta più ampia di Centri di Trasparenza, che include anche analisi delle regole di rilevamento delle minacce e un controllo di verifica per confermare che le build corrispondano alle versioni pubbliche. Nell'ambito della sua Global Transparency Initiative, Kaspersky ha aperto più di 10 strutture di questo tipo in tutto il mondo, offrendo molteplici opzioni di revisione ad aziende ed enti governativi interessati.

Kaspersky è inoltre uno dei soli tre fornitori a garantire l'accesso a una distinta dei componenti software (SBOM) e uno dei soli quattro a pubblicare regolarmente report di trasparenza che descrivono nel dettaglio le richieste provenienti dalle forze dell'ordine e dalle agenzie governative. Questo evidenzia un divario significativo, a livello di settore, tra gli impegni dichiarati e l'effettiva responsabilità pratica.

Kaspersky eccelle tra le pratiche poco adottate

Tra i 60 criteri valutati, Kaspersky ha soddisfatto o superato gli standard di riferimento del settore in 57 categorie, ottenendo il punteggio più alto tra i fornitori esaminati. Inoltre, è stata una delle sole tre aziende a soddisfare tutti i criteri di sicurezza analizzati, tra cui la segnalazione delle vulnerabilità, gli avvisi di sicurezza, la collaborazione e l'impegno alla dichiarazione "Safe Harbor", i risultati degli audit di sicurezza e i processi sicuri del ciclo di vita dello sviluppo del software (SDLC). Nel report, questi elementi sono descritti come "indicatori chiave di affidabilità e resilienza a lungo termine".

La valutazione ha incluso anche un'analisi tecnica pratica dei prodotti per la sicurezza informatica. Durante i test, Kaspersky Next EDR Optimum ha dimostrato una raccolta minima di dati ed è stato riconosciuto per la possibilità offerta ai clienti di disabilitare completamente i servizi di reputazione basati su cloud e la funzionalità EDR.

L'analisi ha inoltre evidenziato come il controllo dei clienti sugli aggiornamenti dei prodotti vari in modo significativo tra i diversi fornitori. Sebbene quasi tutti pubblicino cronologie pubbliche degli aggiornamenti, solo otto supportano l'implementazione graduale e solo sei, tra cui Kaspersky, consentono ai clienti di controllare le definizioni dei virus. Queste funzionalità risultano fondamentali per le organizzazioni che operano in ambienti regolamentati o sensibili, dove sono richieste una gestione rigorosa e la verifica delle modifiche.

Commentando la ricerca, Eugene Kaspersky, Fondatore e CEO di Kaspersky, ha affermato che, per essere credibile, la trasparenza deve essere dimostrabile. Le soluzioni di sicurezza informatica operano in profondità nei sistemi dei nostri clienti, quindi essere responsabili è davvero importante, ha spiegato. "Quando esperti indipendenti esaminano il nostro lavoro, la trasparenza diventa qualcosa di misurabile, non solo una questione di fiducia. Forniamo alle organizzazioni prove concrete su cui basare le proprie decisioni, incoraggiando al contempo standard più elevati in tutto il settore della sicurezza informatica".

Le piattaforme di Endpoint Detection and Response elaborano dati telemetrici, gestiscono aggiornamenti automatici e si affidano a servizi cloud per garantire la protezione. Di conseguenza, trasparenza e responsabilità sono oggi strettamente legate alla governance, alla conformità e ai rischi della catena di fornitura, piuttosto che essere considerate esclusivamente attributi tecnici.

La trasparenza è un fattore determinante

Il report conclude che, per i CISO e gli stakeholder aziendali, la trasparenza dovrebbe rappresentare un criterio fondamentale nella selezione dei fornitori. Le aziende che combinano una protezione efficace

con una trasparenza strutturata, come la disponibilità di SBOM, processi di aggiornamento verificabili, risultati di audit pubblicati e flussi di dati controllabili dai clienti, offrono un livello di garanzia più elevato.

A livello industriale, la ricerca riflette un cambiamento più ampio verso una governance della sicurezza informatica basata sulla responsabilità. Le iniziative normative pongono sempre maggiore enfasi su tracciabilità, sviluppo sicuro e trasparenza post-commercializzazione, indicando che pratiche oggi considerate poco diffuse potrebbero presto diventare standard di base. Le valutazioni indipendenti forniscono quindi un punto di riferimento sia per i fornitori sia per i clienti, man mano che queste aspettative evolvono.

Per supportare i CISO nella gestione dei rischi legati alle terze parti, Kaspersky ha incluso nel white paper una checklist pratica che consente di valutare l'affidabilità dei fornitori di software e rafforzare la resilienza della catena di approvvigionamento.

Il report completo, "Transparency Review and Accountability in Cybersecurity", è disponibile al seguente link.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Responsabilità editoriale di Kaspersky

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Gennaio 19, 2026

Autore

redazione