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

Descrizione

COMUNICATO STAMPA â?? 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 responsabilitÃ di 14 fornitori leader nel settore della sicurezza informatica. Dallo studio, Kaspersky emerge come uno dei fornitori piÃ¹ trasparenti analizzati, superando costantemente gli standard di settore in materia di trattamento dei dati, affidabilitÃ della catena di fornitura e capacitÃ di verifica da parte dei clienti.

Lo studio indipendente Transparency Review and Accountability in Cyber Security (Trasparenza, revisione e responsabilitÃ nella sicurezza informatica), su cui si basa il white paper di Kaspersky, Ã¨ stato commissionato dalla Wirtschaftskammer Ã?sterreich (WKO) e condotto da MCI | The Entrepreneurial SchoolÂ® ed esperti legali, in collaborazione con AV-Comparatives. La ricerca valuta i fornitori sulla base di unâ??ampia gamma di criteri di trasparenza e responsabilitÃ e rileva che, sebbene la conformitÃ 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 Ã¨ risultata uno dei soli tre fornitori, su 14 valutati, a offrire ai propri clienti lâ??accesso a Centri di Trasparenza, dove Ã¨ 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 lâ??offerta piÃ¹ ampia di Centri di Trasparenza, che include anche lâ??analisi delle regole di rilevamento delle minacce e un controllo di verifica per confermare che le build corrispondano alle versioni pubbliche. Nellâ??ambito della sua Global Transparency Initiative, Kaspersky ha aperto piÃ¹ di 10 strutture di questo tipo in tutto il mondo, offrendo molteplici opzioni di revisione ad aziende ed enti governativi interessati.

Kaspersky Ã¨ inoltre uno dei soli tre fornitori a garantire lâ??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 dellâ??ordine e dalle agenzie governative. Questo evidenzia un divario significativo, a livello di settore, tra gli impegni dichiarati e lâ??effettiva responsabilitÃ 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 piÃ¹ alto tra i fornitori esaminati. Inoltre, Ã¨ stata una delle sole tre aziende a soddisfare tutti i criteri di sicurezza analizzati, tra cui la segnalazione delle vulnerabilitÃ , gli avvisi di sicurezza, la collaborazione e lâ??impegno alla dichiarazione â??Safe Harborâ?•, 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 â??indicatori chiave di affidabilitÃ e resilienza a lungo termineâ?•.

La valutazione ha incluso anche unâ??analisi tecnica pratica dei prodotti per la sicurezza informatica. Durante i test, Kaspersky Next EDR Optimum ha dimostrato una raccolta minima di dati ed Ã¨ stato riconosciuto per la possibilitÃ offerta ai clienti di disabilitare completamente i servizi di reputazione basati su cloud e la funzionalitÃ EDR.

Lâ??analisi ha inoltre evidenziato come il controllo dei clienti sugli aggiornamenti dei prodotti vari in modo significativo tra i diversi fornitori. Sebbene quasi tutti pubblichino cronologie pubbliche degli aggiornamenti, solo otto supportano lâ??implementazione graduale e solo sei, tra cui Kaspersky, consentono ai clienti di controllare le definizioni dei virus. Queste funzionalitÃ 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 profonditÃ nei sistemi dei nostri clienti, quindi essere responsabili Ã¨ davvero importanteâ?•, ha spiegato. â??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 piÃ¹ elevati in tutto il settore della sicurezza informaticaâ?•.

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 responsabilitÃ sono oggi strettamente legate alla governance, alla conformitÃ e ai rischi della catena di fornitura, piuttosto che essere considerate esclusivamente attributi tecnici.

La trasparenza Ã¨ 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 disponibilitÃ di SBOM, processi di aggiornamento verificabili, risultati di audit pubblicati e flussi di dati controllabili dai clienti, offrono un livello di garanzia piÃ¹ elevato.

A livello industriale, la ricerca riflette un cambiamento piÃ¹ ampio verso una governance della sicurezza informatica basata sulla responsabilitÃ . Le iniziative normative pongono sempre maggiore enfasi su tracciabilitÃ , 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 lâ??affidabilitÃ dei fornitori di software e rafforzare la resilienza della catena di approvvigionamento.

Il report completo, â??Transparency Review and Accountability in Cybersecurityâ?•, Ã¨ disponibile al seguente link.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Gennaio 19, 2026
Autore
redazione