Sede operativa e legale:
Kaspersky Lab Italia Srl,
Via Francesco Benaglia, 13 - 00153 Roma
P.IVA e C.F. 09923201009
R.E.A. 1196968

Sede operativa:
Piazza Sigmund Freud, 1
20154, Milano

www.kaspersky.it

Crisi Ucraina - Russia. Dichiarazione Kaspersky

25/02/2022

Gentile Partner,

siamo consapevoli che in questi giorni le preoccupazioni e le domande siano state tante, ed è per questo che vorremmo ribadire alcuni principi e valori fondamentali su cui si basa la nostra Azienda e che ci garantiscono solidità e affidabilità.

In qualità di Azienda globale di cybersecurity, Kaspersky contribuisce all'ecosistema della cybersecurity in Italia e nell'Unione Europea dimostrando grande affidabilità. Kaspersky è un'Azienda privata di livello internazionale, la cui Holding è registrata nel Regno Unito. Le nostre attività locali sono gestite da Entità locali, il che ci dà la possibilità di controllare in modo efficace e indipendente le operazioni internazionali e locali. L'Azienda opera in più di 200 paesi e territori.

Le operazioni aziendali di Kaspersky sono progettate per garantire **un alto livello di resilienza** e **consentire la business continuity nel miglior modo possibile**. Ciò viene garantito da una distribuzione equilibrata di compiti e responsabilità tra la Sede centrale e le Entità legali nelle diverse regioni. L'Azienda garantisce l'adempimento dei suoi obblighi verso i Partner e i Clienti, compresa la consegna e il supporto dei prodotti e la continuità delle transazioni finanziarie.

Dal 2008 il nostro modello operativo si basa su un sistema finanziario diversificato. Le nostre Entità locali agiscono indipendentemente in termini di operazioni finanziarie. Ogni Entità legale locale ha le proprie entrate e gestisce direttamente le relazioni con i Partner. Ciò significa che le nostre transazioni commerciali e la fatturazione con i Partner e i Clienti regionali sono gestite dalle Entità legali locali, con conti bancari in Banche locali che non possono essere soggette a nessun impatto negativo in caso di disconnessione da SWIFT.

Grazie all'iniziativa GTI, Kaspersky migliora costantemente il livello di fiducia e responsabilità nei suoi confronti da parte del settore della cybersecurity e fornisce ai suoi Clienti e Partner passi chiari per una maggiore garanzia di sicurezza nelle sue soluzioni. In particolare, Kaspersky ha implementato le seguenti misure:

- **Trasferimento dell'elaborazione e dell'archiviazione dei dati in Svizzera**. Abbiamo costruito un'infrastruttura di dati in due data center situati a Zurigo per l'elaborazione e l'archiviazione dei dati relativi alle minacce informatiche dei nostri clienti in Europa, Stati Uniti e Canada, così come diversi Paesi dell'Asia-Pacifico.
- **Creato una rete globale di Transparency Centers** per la revisione del nostro codice sorgente, di tutte le versioni delle nostre build e dell'AV-database, dello sviluppo del software e della gestione dei dati - incluse le revisioni dei tipi di informazioni che, generalmente, i prodotti Kaspersky inviano al nostro Kaspersky Security Network (KSN) basato su cloud. Inoltre, forniamo anche l'accesso al nostro codice sorgente per ricostruirlo e assicurarsi che corrisponda ai moduli disponibili al pubblico. Kaspersky

fornisce anche una distinta dei materiali software (SBOM) per i suoi prodotti. I nostri Transparency Center si trovano a Zurigo (Svizzera), Madrid (Spagna), Kuala Lumpur (Malesia), San Paolo (Brasile) e New Brunswick (Canada).

- **Abbiamo confermato la sicurezza e l'affidabilità delle nostre pratiche ingegneristiche e dei data service con due rigorose valutazioni di terze parti**. Abbiamo superato con successo l'audit SOC 2 (Service Organization Control for Service Organizations) Type 1 da parte di uno dei revisori delle Big Four, che ha confermato i controlli di sicurezza nel processo di sviluppo e rilascio degli aggiornamenti AV di Kaspersky contro il rischio di modifiche non autorizzate. Abbiamo anche ricevuto la certificazione per i nostri data service per la conformità allo standard ISO/IEC 27001:2013 da parte di TÜV AUSTRIA.
- **Programma di gestione delle vulnerabilità**. Nel marzo 2018, abbiamo aumentato le ricompense per qualsiasi falla critica trovata nei nostri prodotti fino a $100k tramite il nostro programma Bug Bounty. Da allora abbiamo assegnato 53 segnalazioni di vulnerabilità, anche se non sono mai state segnalate vulnerabilità critiche. Con questo approccio avanzato di gestione e divulgazione delle vulnerabilità siamo in grado di rendere i nostri prodotti sempre più sicuri. Per fornire anche una maggiore trasparenza nella gestione delle vulnerabilità, Kaspersky ha svelato i suoi Five Ethical Principles for Responsible Vulnerability Disclosure.

Le operazioni commerciali di Kaspersky rimangono stabili.
Il team di Management globale sta tenendo monitorata la situazione con estrema attenzione ed è pronto ad intervenire celermente se necessario.

Kaspersky Lab rimane disponibile a supportarTi e, in caso di domande o dubbi, sentiti libero di contattarci.

Cordiali saluti,

Cesare D'Angelo
General Manager Italia, Kaspersky