Kaspersky e le garanzie di affidabilità nei momenti di crisi

intervista a Cesare D'Angelo, General Manager di Kaspersky Italia | a cura di Raffaello Juvara

Partiamo dalla domanda d'obbligo in questo momento di crisi. In merito alle preoccupazioni che in occidente tutti hanno rispetto ad un'ipotetica azione coercitiva da parte del governo di Mosca nei confronti di una società privata come Kaspersky che, comunque è russa, cosa rispondete?

Faccio una piccola premessa perché, giustamente, hai parlato di una società russa. In realtà, per quanto la sede e l'origine dell'azienda siano in Russia, Kaspersky è un'azienda globale con la capogruppo registrata a Londra da ormai più di vent'anni. Di fatto, oggi non si può parlare di un'azienda solo russa ma di una multinazionale a tutti gli effetti con la capogruppo registrata, appunto, in UK.

Per rispondere alla tua domanda, quello che abbiamo fatto da tempo e che è ancora più importante ribadire in questa situazione, è stata l'adozione di processi sia per lo sviluppo delle soluzioni che per il loro controllo che ci portano a dire che oggi un'azione coercitiva da parte di un qualsiasi governo difficilmente avrebbe successo per diversi motivi.

Intanto, perché il nostro CEO ha già dichiarato, in più occasioni che, qualora dovesse essere in qualche maniera spinto o obbligato dal governo a mettere in piedi determinate azioni, la sua risposta sarebbe negativa.

Da un'altra parte, ci sono processi e dati oggettivi con tanto di certificazioni, che aiutano a capire come questo sarebbe veramente difficile da realizzare.

Abbiamo spostato da tempo in Svizzera i nostri data center che processano le informazioni che arrivano su base volontaria da parte dei clienti. A Zurigo abbiamo il "Transparency Center", il luogo fisico dove i clienti governativi e le aziende accreditate, dopo una selezione a valle della loro richiesta, possono ispezionare il codice sorgente del prodotto e capire come vengano gestiti i

processi di sviluppo del software e gli aggiornamenti prima che vengano distribuiti ai clienti.

Per questo Transparency Center abbiamo ottenuto due certificazioni da parte di analisti esterni.

Una delle "Big Four" ha rilasciato la certificazione SoC di livello 2 ai nostri processi di scrittura, aggiornamento e distribuzione del software, avendo rilevato la conformità agli standard di sicurezza previsti da questo format, mentre TUV Austria ha rilasciato la certificazione ISO 27001 per la qualità di gestione dei dati dei clienti.

Ultimamente, anche il Garante della Privacy in Italia ha aperto un'istruttoria per capire come noi gestiamo i dati dei nostri clienti. Abbiamo risposto al Garante nei tempi dovuti dando tutte le informazioni richieste e siamo confidenti che venga confermato anche ufficialmente il rispetto delle norme sul trattamento dei dati dei clienti.

In sintesi, le soluzioni di cui stiamo parlando oggi, che sono tipicamente soluzioni di "endpoint protection" o antivirus come vengono chiamate più comunemente, garantiscono

ai nostri clienti che non si possono trasformare da strumento di difesa a strumento in attacco, come gli enti esterni hanno certificato relativamente ai processi con cui questi prodotti vengono poi portati sul mercato.
Non da ultimo, questi processi sono stati pensati e realizzati in modo che, prima di arrivare sui device dei nostri clienti, tutti gli aggiornamenti vengano lavorati, analizzati e verificati in più step, in più country. Il passaggio finale, prima della distribuzione ai nostri clienti, viene fatto fuori dalla Russia.
Quindi pensare oggi che ci possa essere da un momento all'altro una modifica del nostro software per portare un attacco o, come alcuni sostengono, per tralasciare qualche verifica e far passare qualche cosa che non dovrebbe passare, è veramente un'ipotesi molto remota.

Remota significa però che non è impossibile, che non si può escludere completamente…
Questo è, in realtà, un problema generale dal momento che tutti i sistemi, avendo accesso ad ogni file del computer, potrebbero diventare degli strumenti in grado di fare qualcosa di diverso rispetto a quello per cui sono stati pensati.
Nel nostro caso, l'ipotesi che viene discussa più spesso è che da un giorno all'altro qualcuno si presenti in ufficio e ordini che il prodotto debba diventare un "attaccante" o che passi delle informazioni. È uno scenario che, se si dovesse verificare, richiederebbe settimane, mesi o addirittura anni, dal momento che oggi il nostro prodotto è basato su miliardi di interazioni quotidiane. Abbiamo 400 milioni di utenti sparsi in tutto il mondo e parte di questi utenti ha deciso di condividere le proprie informazioni alimentando il motore nel cloud basato su algoritmi di intelligenza artificiale che, negli anni, ha raggiunto la capacità di distinguere ciò che è malevolo da quello che non lo è, di segregarlo e di neutralizzarlo. E' pertanto impossibile che dal mattino al pomeriggio qualcuno decida di modificare questo motore e, se dovesse mai succedere, sarebbe comunque un lavoro che richiedebbe tempo e verrebbe in qualche modo intercettato.

Nella sostanza, tu affermi che chi sia eventualmente esposto a questo tipo di rischio avrebbe tempo e modo di potersi difendere e mettersi in sicurezza, giusto?
Diciamo che se anche qualcuno a monte del processo intendesse modificare il perimetro, a valle di quella modifica sono previsti dei controlli finalizzati ad annullare le modifiche fatte a monte proprio sulla base di quei processi che sono stati certificate, come ti ho spiegato. E questo era stato fatto già in tempi precedenti il conflitto, proprio per evitare che un ipotetico cybercriminale molto bravo si inserisse nei nostri sistemi e portasse delle modifiche.

Torniamo su un altro tema più generale, che hai toccato prima sottolineando che Kaspersky non è più un'azienda solamente russa ma è un'azienda globale. Parliamo dell'autonomia dei vendor globali rispetto ai governi. Questo passaggio storico sta facendo emergere anche l'esigenza che i fornitori globali possano garantire a tutti gli utilizzatori, siano enti governativi, aziende private o singoli cittadini, la propria autonomia rispetto alle prese di posizione dei governi che, chiaramente possono toccare ambiti più elevati, più sensibili dal punto di vista strategico. Puoi dirci qualcosa su questo tema?
Per come la viviamo e la interpretiamo noi, la sicurezza è un elemento che si basa su tanti attori che lavorano contemporaneamente verso lo stesso obiettivo, per cui la questione della maggiore o minore sovranità di qualche vendor rispetto ad altri è forse più vera a parole che nei fatti. Per esempio, parti delle nostre soluzioni o servizi sono presenti anche in soluzioni o servizi di nostri competitor o di terze parti e sarebbe veramente difficile rimuoverle.
In definitiva, dal punto di vista delle tecnologie, è davvero complicato parlare di autonomia totale.
Poi ogni fornitore ha delle peculiarità che concorrono a una sicurezza globale più solida. Quando parliamo ad esempio di "threat intelligence", le analisi delle minacce informatiche svolte dagli analisti per prevenire gli attacchi dei cybercriminali, noi siamo molto forti nell'analisi e nel contrasto delle minacce che vengono dalla parte est del globo, quindi dall'Asia e dalla Russia. Altri vendor sono invece più presenti e più forti in altre aree, per cui va da sé che mettendo insieme le diverse forze il risultato sia migliore per tutti i clienti.
In definitiva, il mondo digitale si muove con logiche diverse da quelle delle mappe o delle cartine geografiche che hanno dei confini.

Viene difficile pensare che in un mondo in cui si lavora sul cloud - il cui funzionamento e potenza di calcolo non sono necessariamente argomenti di interesse per l'utente finale, a patto che sia rispettato il GDPR - si possa pensare a dei confini come quelli geografici. Lavorando in un mondo globale, dobbiamo essere capaci di attivare al meglio le risorse che arrivano da aziende che hanno una copertura globale, come siamo noi, rispettando tutte le regole legate al trattamento dei dati dei clienti.

A questo punto vorrei farti una domanda in merito ad un altro tema, ovvero la sicurezza delle telecamere, cinesi e non. Adesso il problema è diventato scottante in Italia per la gara Consip ma vorrei analizzarlo da un punto di vista più generale. I timori di diversi governi occidentali, fra cui USA, Gran Bretagna, Australia e, adesso almeno in parte, anche il nostro, riguardano la sicurezza delle telecamere in rete e degli IoT sia sul piano della penetrabilità da parte di estranei che della deviazione dei dati verso destinatari sconosciuti. Come valutate questo problema?

Cercherò di darti una risposta coerente con quello che noi facciamo, rifacendomi a due argomenti.

Da un lato l'argomento tecnico: che si tratti di una telecamera piuttosto che di un registratore di cassa o di qualsiasi altro sensore sul territorio, dal momento in cui è in rete e comunica dati, c'è una vulnerabilità. Noi abbiamo introdotto sul mercato una soluzione che è, appunto, uno "IoT gateway", vale a dire un oggetto che serve a mettere in sicurezza la comunicazione tra i vari sensori sparsi sul territorio e il server centrale al quale devono arrivare le informazioni. Aggiungendo questo "strato", questo livello ulteriore di cybersecurity, mettiamo in sicurezza anche le informazioni che girano tra i vari device e il server che le deve raccogliere rispetto ai possibili attacchi per intercettare questi dati. Quindi, al di là del fatto che si parli di una telecamera cinese piuttosto che di altro, la vulnerabilità e la sicurezza dei dati possono venire gestite e indirizzate.

Poi c'è l'argomento politico che, in questo momento, ci vede sotto i riflettori.

Non entro nel merito se sia giusto o sbagliato puntare il dito su tale fornitore o su tale governo ma, essendo stati tra i primi ad essere oggetto di questo tipo di attenzioni dal 2017 in poi, cosa abbiamo fatto in Kaspersky?

Abbiamo deciso di portare i nostri data center in Svizzera che, oltre ad essere neutrale, è la nazione che all'interno dell'Europa ha le normative più stringenti in termini di data privacy e di sicurezza dei dati dei clienti.

Abbiamo deciso di rendere disponibile, a chi abbia le capacità e l'interesse di farlo, il nostro codice sorgente del prodotto. Questo nell'ottica della massima apertura e trasparenza anche verso le istituzioni governative.

Nel campo della cybersecurity mi risulta che siamo gli unici ad aver fatto un'operazione del genere e non ho evidenza di iniziative simili neanche in altri settori.

Solo dieci giorni fa sono stato a Zurigo con un ospite a far vedere il Transparency Center, qualcosa che si può toccare, si può vedere e si può capire quali garanzie possa dare.

In conclusione, la mia risposta su questo tema è che, al di là delle attenzioni nei confronti di questo o quel governo, c'è modo di rendere affidabili e trasparenti le comunicazioni con i clienti, come abbiamo fatto noi, permettendo di andare a investigare e capire quanto siano sicuri i prodotti.