kaspersky

Disegno di legge recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici

AC 1717

Roma,
Venerdì 5 Aprile 2024

kaspersky

L'AZIENDA

Kaspersky è una delle più grandi multinazionali specializzata nella progettazione e fornitura di *software* per la sicurezza informatica e di digital privacy, che protegge ogni giorno migliaia di istituzioni politiche, sociali, economiche e finanziarie in tutto il mondo, prevenendo il rischio di attacchi cibernetici, con prodotti sicuri, integrati e *customizzati* sulle esigenze dei propri clienti. L'Azienda, che dal 1998 ha sede legale a Londra e che da molti anni offre i suoi servizi anche in Italia con un *focus* sulle grandi imprese, è inoltre attiva con soluzioni *retail*, in *compliance* con le *policy* di trasparenza e sicurezza dei dati, cui si combina un'ulteriore disciplina normativa di settore a carattere interno. Kaspersky, da oltre 25 anni, protegge circa 400 milioni di clienti e 240.000 aziende in tutto il mondo e previene ogni giorno migliaia di *cyber-attacchi*.
In questo contesto si inserisce la ***Global Transparency Initiative***: un'iniziativa – unica nel settore IT – che consente l'ispezione del codice sorgente per la revisione esterna e mette a disposizione di clienti e partner la propria Software Bill of Materials (SBOM), al fine consentire agli stakeholder di conoscere i processi interni e le pratiche di gestione dei dati dell'azienda. .
Kaspersky, comunemente nota per i servizi di *endpoint protection* (c.d. "antivirus"), grazie al presidio dei propri analisti del mondo del *cybercrime* russo, e grazie ai relativi servizi di Threat Intelligence, è *leader* mondiale nel prevenire e sventare attacchi cibernetici provenienti da quella specifica area geografica.

IL CONFLITTO

Kaspersky è stata al centro del dibattito politico nel marzo 2022 a causa delle tragiche vicende connesse all'invasione dell'Ucraina da parte della Russia. Da questo complesso di circostanze è scaturita l'iniziativa regolatoria, con cui – ai sensi dell'art. 29 del decreto-legge 21/2022, è stato chiesto alla Pubblica Amministrazione di avviare un processo di diversificazione dei prodotti offerti dai fornitori "legati alla Federazione Russa". La norma è stata successivamente resa attuativa dalla circolare n. 4336 dell'Agenzia per la Cybersicurezza Nazionale (ACN), del 21 aprile 2022, che citava espressamente Kaspersky all'interno delle aziende "legate alla Federazione Russa", soggette al processo di diversficazione.

LA REAZIONE/IL POSIZIONAMENTO ISTITUZIONALE

L'Azienda ha compreso le misure prese dal Legislatore *pro-tempore*, dando piena disponibilità a collaborare per aiutare le PA a gestire al meglio questo percorso. Da marzo 2022 è stato quindi promossa un'attività informativa e divulgativa finalizzata a far conoscere ai più importanti *stakeholders* istituzionali di riferimento (parlamentari, autorità ed enti governativi) i valori che guidano l'Azienda e la metodologia operativa che si fonda sull'approccio integrato tra rilevazione/analisi della minaccia e creazione di *software* antivirus e *antimalware* per aumentare la resilienza degli apparati tecnologici.

CONTESTO POLITICO NAZIONALE ED EUROPEO

Il dialogo con gli interlocutori parlamentari e le autorità governative si è progressivamente consolidato, grazie anche al garbo "istituzionale" dimostrato dell'Azienda. La valutazione estremamente positiva dei servizi tecnologici offerti, l'indiscutibile affidabilità dei prodotti disponibili in commercio, riconosciute e sottolineate da tutti gli interlocutori che l'Azienda ha incontrato sinora, e l'assenza di un quadro sanzionatorio europeo diretto nei confronti di Kaspersky ha contribuito a distendere il clima generale sulla vicenda. Addirittura in Spagna Kaspersky è tornato ad essere un fornitore consigliato per la Pubblica Amministrazione, come da catalogo del CCN, Centro Criptològico Nacional, aggiornato a febbraio 2024: https://www.ccn-cert.cni.es/es/pdf/guias/series-ccn-stic/guias-de-acceso-publico-ccn-stic/2536-ccn-stic-105-catalogo-de-productos-de-seguridad-de-las-tecnologias-de-la-informacion-y-la-comunicacion/file?format=html.

KASPERSKY OGGI

Sono trascorsi più di due anni dallo scoppio del conflitto e i rischi ipotizzati per i quali era stata emanata la circolare ACN non si sono materializzati. L'Azienda purtuttavia continua ad essere discriminata in ragione dell'invito a diversificare di cui all'art. 29 del decreto-legge 21/2022. Una circostanza che si scontra con la percezione diffusa tra i clienti che l'Azienda rappresenti un ***player* strategico** per investire sulla sicurezza dei propri *asset* informatici. Ad oggi, infattiu, Kaspersky raggiunge costantemente i punteggi migliori nel maggior numero di test indipendenti rispetto a qualsiasi altro fornitore e nel mese di Gennaio 2024 l'Azienda è stata premiata da **AV-Comparatives** come **"Prodotto dell'anno"** per aver garantito costantemente risultati eccezionali per tutto il 2023, con le ultime soluzioni *consumer*.

Kaspersky, in Italia, si è aggiudicata il premio come "**Miglior progetto in ambito Pubblica Amministrazione**" fra le proposte che si sono candidate all'edizione 2022 degli **Italian Project Awards** (#IPA2K22). Il premio aggiudicato è stato conferito nell'ambito del CitySCAPE, un progetto cofinanziato dalla Commissione Europea, coordinato dall'Istituto di Comunicazioni e Sistemi Informatici di Atene (ICCS), che vede coinvolto un consorzio di 15 partner, tra cui l'Azienda Mobilità e Trasporti di Genova (AMT) e il Consiglio dei Trasporti della Città di Tallinn. La giuria ha motivato il premio spiegando che questo progetto è "*in grado di esplorare e valorizzare alcune dimensioni della sicurezza informatica applicate al trasporto multimodale mediante l'utilizzo di tecnologie innovative e allo stesso tempo di valorizzare il fattore umano attraverso contenuti formativi a fine di accrescere il livello di competenza in materia di sicurezza dei dati degli utilizzatori*".

MINACCE IN AUMENTO

Il recente "**Rapporto 2024 sulla sicurezza ICT in Italia**", report annuale redatto dal CLUSIT – Associazione Italiana per la Sicurezza Informatica, evidenzia come tra gennaio 2019 e dicembre 2023 si siano verificati un totale di 10.858 cyber attacchi, con un aumento nel 2023 del 12% circa sul 2022. Il Clusit, oltre a registrare la cifra record di 2.779 incidenti nell'ultimo anno (2023), evidenzia come gli eventi degli

ultimi cinque anni (2019-2023) siano più della metà (56.3%) degli incidenti in totale dal 2011, a conferma di una costante recrudescenza dello scenario degli incidenti.

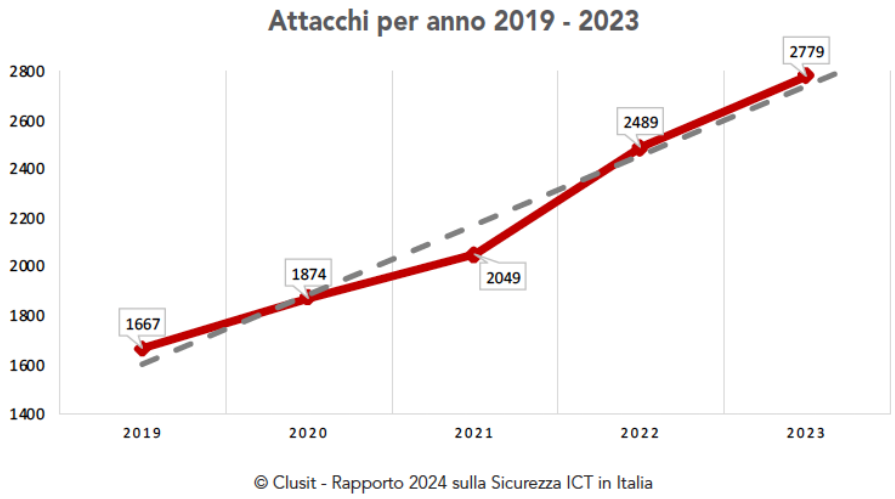

Fig. 1 - Andamento dei cyber attacchi nel periodo 2019-23

LA PROPOSTA

L'Azienda manifesta grande apprezzamento per l'iniziativa legislativa del Governo che ha portato alla predisposizione del disegno di legge in oggetto recante disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici, condividendo sia l'impianto regolamentare che i principi sanzionatori. Consapevoli che i danni provenienti da attacchi cyber si propagano molto velocemente, è importante agire tempestivamente per identificare e isolare le minacce, e in questa attività il partner tecnologico a cui ci si affida gioca un ruolo fiondamentale. Particolarmente condivisibile la previsione normativa di cui all'articolo 6, con cui viene istituito in tutte le amministrazioni il "referente per la cybersicurezza" quale figura incaricata al controllo, alla supervisione nonché all'implementazione di tutta la normativa di settore.

Peraltro, a fronte di un aumento consistente degli attacchi cyber rilevati nel 2023 – come evidenziato dall'ultimo rapporto Clusit – Kaspersky propone di rivedere e superare quanto disposto dal decreto-legge 21 marzo 2022, n. 21, recante "*Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina*", con il quale – all'articolo 29 "Rafforzamento della disciplina cyber" – si invitano le Pubbliche Amministrazioni a diversificare le forniture di servizi software provenienti da aziende legate alla Federazione Russa. In virtù delle crescenti instabilità geopolitiche a cui stiamo assistendo e condividendo le finalità del provvedimento in oggetto, si propone di incrementare i livelli di cybersicurezza richiesti, delegando all'Agenzia per Cybersicurezza Nazionale (ACN) il potere di certificare l'idoneità delle aziende fornitrici di software e servizi informatici alla pubblica amministrazione, incrementando il criterio della provenienza geografica di detti fornitori.

kaspersky

AC 1717
Emendamento

Art 10
Dopo l'articolo, aggiungere il seguente:

Art. 10-bis.
(*Modifiche all'articolo 29 del decreto-legge 21 marzo 2022, n. 21*).

1. All'articolo 29 del decreto-legge 21 marzo 2022, n. 21, succ. modd., sono apportate le seguenti modificazioni:
a) al comma 1, dopo le parole "prodotti appartenenti alle categorie individuate al comma 3," sono aggiunte le seguenti "nonché dei prodotti e servizi non dotati della certificazione di cui ai commi 3-*bis* e 3-*ter,* ";
b) dopo il comma 3, sono aggiunti i seguenti:
"3-bis. La circolare di cui al comma 3 definisce altresì le modalità e i criteri specifici per il rilascio della certificazione da parte dell'Autorità per la cybersicurezza nazionale, ai sensi del comma 3-ter.
3-ter. L'Agenzia per la cybersicurezza nazionale certifica le aziende dotate di specifici requisiti di sicurezza tecnologica indipendenti dalla provenienza geografica e di procedure e protocolli atti a prevenire pregiudizi alla sicurezza di reti, sistemi informativi e servizi informatici delle amministrazioni pubbliche, ai sensi del presente articolo.
3-quater. La circolare di cui al comma 3, oltre ai prodotti e servizi ivi menzionati, ricomprende i prodotti e servizi delle aziende certificate ai sensi dei commi 3-bis e 3-ter. A tal fine, l'Agenzia per la cybersicurezza nazionale provvede annualmente all'aggiornamento della circolare."

2. L'Agenzia per la cybersicurezza nazionale provvede all'aggiornamento della circolare di cui al comma 3 dell'articolo 29 del decreto-legge 21 marzo 2022, n. 21, ai sensi del presente articolo, entro e non oltre 2 mesi dall'entrata in vigore della presente legge.

Relazione illustrativa
A fronte di un aumento consistente degli attacchi cyber rilevati negli ultimi anni, nonché alla luce delle crescenti instabilità geopolitiche a cui stiamo assistendo, si propone di rivedere e superare quanto disposto dall'art. 29 del decreto-legge 21 marzo 2022, n. 21, recante "Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina", rafforzando il ruolo dell'ACN nel certificare l'idoneità delle aziende fornitrici di software e servizi informatici alla Pubblica Amministrazione, indipendentemente dalla provenienza geografica delle aziende. Si tratta di un intervento molto simile a quello realizzato dalla Spagna per elevare i livelli di standard qualitativi e di sicurezza nazionale.
L'intervento non reca nuovi oneri a carico della finanza pubblica.