di Roxy Tomasicchio

Italia Oggi, 23 novembre 2021

A livello mondiale il cybercrime divora il 6% del Pil. Gli attacchi verso l'Europa erano l'11% due anni fa, oggi sono il 25% del totale. Nel primo semestre sono stati 1.053 quelli gravi, il 24% in più rispetto allo stesso periodo del 2020. L'allarme lanciato dal rapporto Clusit 2021.

Si affina la tecnica dei pirati informatici: gli attacchi diventano mirati, per obiettivo e area geografica, e le tecniche diventano sempre più efficaci, tanto che crescono gli attacchi classificati come gravi. Trasformando le parole in cifre: nei primi sei mesi del 2021, il 25% degli attacchi mappati è stato diretto verso l'Europa (senza contare gli attacchi multipli); nel 2020 la quota era al 17% ed era all'11% nel 2019. Sono stati 1.053 gli attacchi gravi, cioè quelli con un impatto in diversi aspetti della società, della politica, dell'economia e della geopolitica.

È il 24% in più rispetto allo stesso periodo del 2020, con una media mensile pari a 170 attacchi, contro i 156 del 2020. Una crescita comunque sottostimata, se si considera che il campione comprende solo gli attacchi denunciati e resi noti. A delineare il quadro è la nuova edizione del rapporto Clusit 2021, presentata nel corso di Security Summit Streaming Edition, l'evento di riferimento per la cybersecurity in Italia organizzato da Clusit, Associazione italiana per la sicurezza informatica, con Astrea, agenzia specializzata nell'organizzazione di eventi nell'ambito della sicurezza informatica. Siamo, secondo gli esperti dell'associazione, in una emergenza globale: le perdite stimate per le falle della cybersecurity sono pari a 6 trilioni di dollari per il 2021 e incidono ormai per una percentuale significativa del Gdp mondiale (oltre il 6%), con un tasso di peggioramento annuale a 2 cifre e un valore pari a 3 volte il Pil italiano.

Cosa sta succedendo, in particolare in Italia ed Europa? Forse i criminali hanno scoperto che è più redditizio attaccare qui rispetto ad altre zone del mondo? "Io non credo", spiega Gabriele Faggioli, presidente Clusit, "penso che in realtà i dati derivino da altri elementi e in particolare dalla spinta delle normative che hanno costretto chi subisce attacchi che comportano violazioni dei dati a segnalarlo, quando dovuto per legge, non solo alle Autorità ma anche agli interessati oggetto della violazione. Queste comunicazioni agli interessati unitamente al fatto che sempre più spesso i criminali rendono noti gli attacchi soprattutto ransomware fa sì che sia sempre più difficile nascondere i fatti che accadono.

Nel frattempo", aggiunge, "abbiamo una grandissima occasione: il Pnrr e i fondi che saranno riversati in innovazione digitale nei prossimi anni. Al di là del capitolo di spesa specifico, si deve pensare a tutto il resto. Non esiste innovazione senza sicurezza". Gli ha fatto eco Andrea Zapparoli Manzoni, co-autore del rapporto Clusit e membro del comitato direttivo Clusit: "Da anni siamo di fronte a problematiche che per natura, gravità e dimensione travalicano costantemente i confini dell'Ict e della stessa cybersecurity. Auspichiamo che il Pnrr, che complessivamente alloca circa 45 miliardi di euro per la transizione digitale, possa rappresentare per l'Italia l'occasione di mettersi al passo e colmare le proprie lacune anche in ambito cyber".

I dati. Sono cresciuti del 21% gli attacchi gravi compiuti per finalità di cybercrime, ossia per estorcere denaro alle vittime, e oggi rappresentano l'88% del totale. Mentre sono aumentati del 18% gli attacchi riferibili alla cosiddetta "guerra delle informazioni", la information warfare. Calano, invece, quelli classificati come attività di cyber espionage, spionaggio cibernetico, (-36,7%), dopo il picco straordinario del 2020 dovuto principalmente allo spionaggio relativo allo sviluppo di vaccini e cure per il Covid-19.

Nel rapporto si misura la cosiddetta "severity" degli attacchi, cioè la gravità secondo quattro categorie. Le variabili sono molteplici e includono l'impatto geopolitico, sociale, economico (diretto e indiretto) e di immagine. Nel primo semestre 2021 gli attacchi gravi con effetti "molto importanti" e "critici" sono il 74% del totale (erano il 49% nel 2020). Il 22% degli attacchi analizzati sono di impatto significativo, quelli con impatto basso solo il 4%.

In merito agli obiettivi, in termini assoluti, rispetto al secondo semestre 2020, da gennaio a giugno 2021 si osserva l'incremento più elevato degli attacchi gravi nelle categorie: trasporti e stoccaggio (transportation / storage, +108,7%), servizi professionali, scientifici e tecnici (professional, scientific, technical, +85,2%) e informazione e multimedia (news & multimedia, +65,2%), seguite da commercio all'ingrosso e dettaglio (wholesale / retail, +61,3%) e produzione manifatturiera (manufacturing, +46,9%). Aumentano anche gli attacchi verso le

categorie energia e servizi pubblici (energy / utilities, +46,2%), settore pubblico (government, +39,2%), arti e intrattenimento (arts / entertainment, +36,8%) e sanità (healthcare, +18,8%)

La categoria dei bersagli multipli, i multiple targets (si tratta di attacchi gravi compiuti in parallelo dallo stesso gruppo di attaccanti contro numerose organizzazioni appartenenti a categorie differenti), registra invece una diminuzione del 23,4% rispetto al secondo semestre 2020. Siamo di fronte a un cambio di strategia da parte degli attaccanti rispetto allo scorso anno: secondo gli esperti Clusit l'aumento di attacchi gravi mirati verso singoli bersagli rappresenta un importante campanello di allarme, in particolare perché caratterizzati da tecniche di tipo ransomware con l'aggravante della "double extortion", la doppia estorsione, cioè della minaccia di diffondere i dati rubati alle vittime qualora non paghino il riscatto.

In termini percentuali la categoria government rappresenta il 16% del totale e si conferma al primo posto, come nel precedente semestre. Al secondo posto, ancora la sanità, con il 13% degli attacchi totali, e al terzo i multiple targets, che in questo semestre rappresentano il 12% delle vittime.

Sotto l'aspetto delle tecniche di attacco, secondo gli esperti Clusit, gli attaccanti possono ancora fare affidamento sull'efficacia del malware, prodotto industrialmente a costi decrescenti, e sullo sfruttamento di vulnerabilità note, per colpire più della metà dei loro obiettivi, ovvero il 59% dei casi analizzati.

Il malware, quindi, è la categoria che nei primi sei mesi di quest'anno mostra numeri assoluti maggiori: rappresenta infatti il 43% del totale, in crescita del 10,5%. Le tecniche sconosciute sono al secondo posto, in aumento del 13,9% rispetto al secondo semestre 2020, superando la categoria "vulnerabilità note", che è per altro in preoccupante crescita (+41,4%). Il 22% di attacchi realizzati con "tecniche sconosciute" (che crescono del 13,9%) è dovuto al fatto che un quinto degli attacchi diventano di dominio pubblico a seguito di un data breach: in questo caso, le normative impongono una notifica agli interessati, ma non di fornire una descrizione precisa delle modalità dell'attacco.