Kaspersky: le telecomunicazioni sono i primi bersagli dei cyberattacchi nel 2024

Milano, 1 agosto 2024

Secondo Kaspersky, telecom, mass media e società di costruzioni sono i principali bersagli dei cyberattacchi nella prima metà del 2024. Le telecomunicazioni hanno subito il maggior numero di incidenti, probabilmente a causa dell'interesse degli aggressori per i dati sensibili e lo sfruttamento delle relazioni di fiducia. A loro volta, i mass media sono tradizionalmente presi di mira durante i conflitti internazionali, mentre le società di costruzioni possono essere interessanti perché si affidano a numerosi subappaltatori.

In base alle stime di Kaspersky Managed Detection and Response (MDR), da gennaio a giugno 2024 nel settore delle telecomunicazioni si sono verificati 284 incidenti di cybersicurezza ogni 10.000 sistemi. Le aziende che si occupano di mass media hanno subito 180 attacchi ogni 10.000 sistemi, mentre i settori delle costruzioni, alimentare e industriale seguono rispettivamente con 179, 122 e 121 incidenti.

"Un attacco riuscito, soprattutto se avanzato, a un'azienda di telecomunicazioni può esporre i dati di milioni di clienti, compresi dettagli di contatto e le informazioni sulle carte di credito. Inoltre, può servire da trampolino di lancio per ulteriori attacchi ai clienti attraverso lo sfruttamento di relazioni di fiducia. Ecco perché questo settore è così interessante per i criminali informatici. Le organizzazioni dei mass media, a loro volta, diventano un obiettivo sempre più frequente durante i conflitti internazionali, spesso caratterizzati da una vera e propria guerra dell'informazione in cui svolgono un ruolo cruciale. Infine, ma non meno importante, le imprese di costruzioni hanno volumi di denaro significativi e si affidano a subappaltatori, rendendoli vulnerabili agli attacchi tramite infrastrutture di partner fidati e spear phishing", **ha dichiarato Sergey Soldatov, Head of Kaspersky Managed Detection and Response.**

Le telco hanno anche affrontato il più alto numero medio di incidenti critici, con 32 attacchi ogni 10.000 sistemi. *"Gli incidenti critici sono attacchi provocati dall'uomo o minacce malware che hanno un impatto significativo potenziale o effettivo sull'infrastruttura aziendale",* **ha spiegato Sergey Soldatov.** L'IT segue con quasi 12 incidenti critici medi, mentre il settore governativo ha registrato otto incidenti critici medi nella prima metà del 2024.

A livello globale, il numero di incidenti informatici è rimasto relativamente stabile, con una leggera diminuzione. Le organizzazioni tendono a rafforzare le proprie misure di sicurezza informatica dopo l'impennata degli attacchi nel 2021-2022. Approcci più incisivi come la valutazione delle vulnerabilità e i test di penetrazione hanno migliorato la sicurezza complessiva. *"I cyberattacchi rispecchiano tipicamente i conflitti globali, soprattutto quelli determinati dall'uomo. L'intensificarsi del panorama delle minacce nel periodo 2021-2022 ha portato a una maggiore attenzione alla cybersecurity da parte delle imprese e delle organizzazioni in vari ambiti, con conseguenti livelli di sicurezza più elevati grazie all'apprendimento dalle esperienze passate",* **ha aggiunto Sergey Soldatov.**

Per proteggere le imprese dalle minacce informatiche, Kaspersky raccomanda le seguenti misure:

- Implementare il servizio di Managed Detection and Response (MDR) per individuare in modo proattivo le minacce.

- Per assicurarsi che l'infrastruttura non sia stata violata, condurre periodicamente una valutazione della compromissione e, in caso di prove evidenti di un attacco informatico, avviare una risposta agli incidenti.
- Per sviluppare le proprie procedure di sicurezza interne, i servizi di consulenza SOC possono essere d'aiuto.
- Fornire al proprio team SOC l'accesso alle informazioni più recenti sulle minacce (TI). Kaspersky Threat Intelligence Portal è un unico punto di accesso per le informazioni sulle minacce dell'azienda, che fornisce dati sui cyberattacchi e approfondimenti raccolti da Kaspersky in oltre 20 anni.
- Aggiornare il proprio team di cybersecurity per affrontare le più recenti minacce mirate con Kaspersky Expert Training (xTraining) sviluppato dagli esperti del GReAT.
- Oltre ad adottare una protezione essenziale degli endpoint, si deve implementare una soluzione di sicurezza di livello aziendale che rilevi precocemente le minacce avanzate a livello di rete, come Kaspersky Anti Targeted Attack Platform.
- Poiché molti attacchi mirati iniziano con il phishing o altre tecniche di social engineering, è importante organizzare sessioni di formazione sulla consapevolezza della sicurezza e fornire le competenze pratiche, ad esempio attraverso la Kaspersky Automated Security Awareness Platform.

Informazioni su Kaspersky

Kaspersky è un'azienda globale di sicurezza informatica e digital privacy fondata nel 1997. Le profonde competenze in materia di Threat Intelligence e sicurezza si trasformano costantemente in soluzioni e servizi innovativi per proteggere aziende, infrastrutture critiche, governi e utenti in tutto il mondo. Il portfolio completo di sicurezza dell'azienda comprende una protezione leader degli endpoint e diverse soluzioni e servizi di sicurezza specializzati e soluzioni Cyber Immune, per combattere le sofisticate minacce digitali in continua evoluzione. Oltre 400 milioni di utenti sono protetti dalle tecnologie Kaspersky e aiutiamo 220.000 aziende a tenere al sicuro ciò che più conta per loro. Per ulteriori informazioni è possibile consultare https://www.kaspersky.it/

Seguici su:

https://twitter.com/KasperskyLabIT
http://www.facebook.com/kasperskylabitalia
https://www.linkedin.com/company/kaspersky-lab-italia
https://www.instagram.com/kasperskylabitalia/
https://t.me/KasperskyItalia

Contatto di redazione:

Noesis

Cristina Barelli, Silvia Pasero,
Eleonora Bossi

kaspersky@noesis.net

Kaspersky Italia
Alessandra Venneri
Head of Corporate Communications & Public Affairs Italy
Piazza Sigmund Freud, 1 - Milano
alessandra.venneri@kaspersky.com