State of cybersecurity: Gennaio - Giugno 2023

I recenti attacchi informatici confermano che la sicurezza delle aziende è costantemente messa alla prova da nuove tipologie di minacce.

Avere dati tangibili sull'andamento della sicurezza informatica all'interno della propria infrastruttura aziendale è fondamentale per adattare le strategie di difesa.

Il seguente report si basa su un campione di 180 aziende italiane monitorate all'interno della piattaforma MDR Certego PanOptikon®.

Ha l'obiettivo di confrontare i volumi di attacco dei primi mesi del 2023 con lo stesso periodo dell'anno precedente e analizzare l'evoluzione dello stato di sicurezza delle aziende italiane.

ASSET MONITORATI
(campione di ricerca)

1.283.519

Endpoints, networks, cloud, OT environments e vulnerabilities monitorate all'interno della piattaforma MDR Certego PanOptikon®

2022 Gennaio - Giugno		2023 Gennaio - Giugno
2.960.799	EVENTI DI CYBERSECURITY	2.366.273

Eventi grezzi di telemetria processati dalla piattaforma MDR Certego PanOptikon®

64.080	ALLARMI	91.250

Eventi di cybersecurity che hanno passato le linee di difesa preventive e che in seguito all'applicazione automatica di regole di Threat Intelligence, tecniche di Behavioral Analytics e tecnologie di AI e Machine Learning, hanno generato un allarme all'interno della piattaforma MDR.

+42% rispetto all'anno precedente

6.016	INCIDENTI	8.491

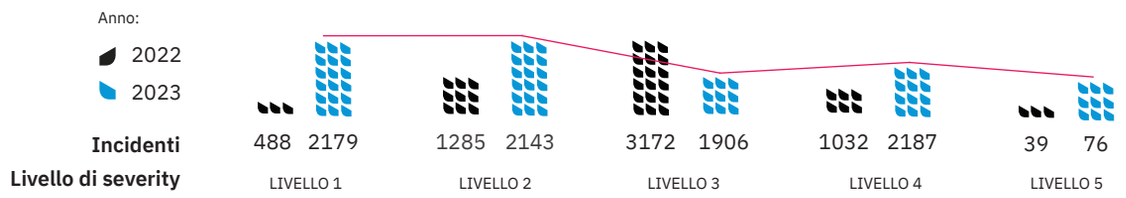
Allarmi che in seguito alle attività di analisi del Detection & Response Team di Certego, hanno generato un ticket di sicurezza all'interno della piattaforma, che ha richiesto la collaborazione con il reparto IT del cliente per le attività di mitigazione.

+41% rispetto all'anno precedente

State of cybersecurity: Gennaio - Giugno 2023

SEVERITY DEGLI INCIDENTI

La severity degli incidenti viene concordata in fase di deployment con il cliente. Rappresenta il livello di pericolosità di un Incidente in relazione all'asset a cui è collegato e alle esigenze di business dell'organizzazione.

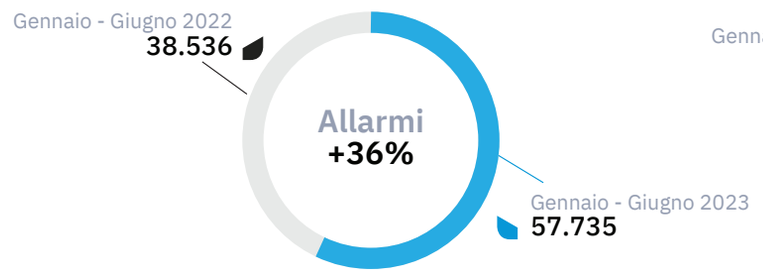


Rispetto all'anno precedente, il 2023 registra un aumento dei ticket di severity 4 e 5; i criminali informatici riescono ad individuare più facilmente gli asset prioritari per le organizzazioni.

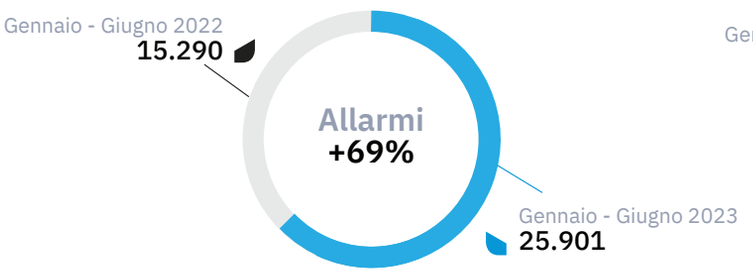
SUPERFICI DI ATTACCO

In particolare, i primi 6 mesi del 2023 registrano un elevato aumento dei tentativi di attacco verso gli apparati network e dispositivi endpoint

Apparati NETWORK



Dispositivi ENDPOINT



AUMENTO PER SETTORE MERCEOLOGICO

Chemical/Pharmaceutical	+28%
Educational/Research	+60%
Energy/Environment	+50%
Fashion/Design	+37%
Finance/Insurance	+2%
GDO/Retail	+2,5%
Healthcare	+40%
IT Services	+8%
Manufacturing/Industry	+35%
Public Administration	+20%

Rispetto all'anno precedente, con valore riproporzionato sul numero di asset monitorati, si riscontra un aumento degli eventi di sicurezza per tutti i settori merceologici monitorati.
In particolare:

Educational, Energy, Healthcare e Manufacturing rappresentano gli ambiti di imprese che hanno registrato un più esponenziale incremento degli attacchi rispetto all'anno precedente.

Focus Points

- **Il 2023 conferma che le sole strategie di prevenzione non possono più essere sufficienti. Rispetto all'anno precedente sono infatti aumentati del 42% gli episodi di sicurezza che sono riusciti a passare le prima linee di difesa.**
- **Senza il ricorso a strategie e soluzioni di sicurezza in grado di filtrare e gestire in maniera automatizzata specifiche tipologie di attacchi, i reparti IT dovrebbero destinare quasi la totalità delle risorse alla gestione degli incidenti, a discapito delle attività più strettamente correlate al business aziendale.**
- **Aumenta il livello di severità degli attacchi, che sempre di più, colpiscono gli asset critici aziendali.**
- **Non c'è settore merceologico immune agli attacchi informatici. Anche le aziende strettamente meno correlate al digitale rappresentano un target per i criminali informatici.**

You can't schedule a cyberattack, but you can be ready for it!

Via F. Lamborghini 81, 41121 Modena (MO)