ARTICOLO DI ELEARNINGNEWS

Year 5 - number 171 Wednesday 8 september 2021

Cybersecurity aziendale: i dati sugli attacchi

Un incidente ogni 10 analizzati ha un livello di gravità alto

Secondo i metadati anonimi forniti volontariamente dai clienti **Kaspersky MDR**, azienda di sicurezza informatica e digital privacy che opera a livello globale da oltre 20 anni, un incidente di cybersecurity su 10 (9%) tra quelli bloccati potrebbe causare gravi interruzioni o accessi non autorizzati alle risorse dei clienti. La maggior parte degli incidenti (72%) era di media gravità.

Abbiamo già visto quali sono i **principali tipi di attacchi informatici** che possono influire sulle prestazioni delle risorse aziendali o portare a casi di uso improprio di dati.

"La ricerca ha mostrato che gli attacchi mirati sono comuni: più di un quarto (27%) delle organizzazioni ne ha subito uno. Quasi tutti i settori, ad eccezione dei mass media e dei trasporti, hanno registrato incidenti di elevata gravità durante il periodo analizzato. Il più delle volte gli incidenti critici hanno colpito organizzazioni del settore pubblico (41%), seguito dal quello IT (15%) e finanziario (13%).

Quasi un terzo (30%) degli incidenti erano relativi ad **attacchi mirati causati dall'uomo** mentre il 23% degli incidenti di elevata gravità è stato classificato come malware ad alto impatto (tra cui i ransomware). Nel 9% dei casi, i criminali informatici hanno ottenuto accesso all'infrastruttura IT aziendale utilizzando tecniche di ingegneria sociale. Le APT attuali sono state rilevate insieme ad artefatti di precedenti attacchi avanzati.

Questo suggerisce che se un'organizzazione risponde a una minaccia sofisticata, viene spesso attaccata una seconda volta, spesso dallo stesso cyber criminale. Inoltre, nelle organizzazioni vittime di APT gli esperti hanno osservato segni di simulazione del comportamento di un avversario, come il red teaming, o una valutazione delle capacità di sicurezza operativa di un'azienda attraverso una sofisticata simulazione di attacco."

La buona notizia è che, essendo a conoscenza dei rischi, si possono avere a disposizione efficaci mezzi per affrontarli, per esempio avvalendosi di servizi dedicati per il rilevamento e il blocco delle minacce, aggiornamento della formazione professionale del team IT, e passaggio importantissimo, ma spesso sottovalutato, **formazione di base sulla sicurezza informatica** di tutto il personale. Infatti, sempre più spesso gli attacchi informatici iniziano con phishing o altre tecniche di ingegneria sociale.